



Product Guide

McAfee Enterprise Security Manager 10.1.0

COPYRIGHT

© 2017 McAfee LLC

TRADEMARK ATTRIBUTIONS

McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, Foundstone, McAfee LiveSafe, McAfee QuickClean, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, TrustedSource, VirusScan are trademarks of McAfee LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION

License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

	Preface	9
	About this guide	9
	Audience	9
	Conventions	9
	Find product documentation	10
	Find localized information	10
1	Introduction	13
	How McAfee® Enterprise Security Manager (McAfee ESM) works	13
	Devices and what they do	14
	Use ESM Help	15
	Find localized information	15
2	Getting started	17
	Log on and off	17
	Customize the logon page	18
	Update ESM software	19
	Obtain and add rule update credentials	19
	Check for rule updates	20
	Change language for event logs	20
	Connecting devices	20
	Add devices to the ESM console	21
	Select a display type	21
	Manage custom display types	22
	Set console timeout value	22
3	Configuring McAfee ESM devices	23
	About device keys	23
	Key a device	23
	Manage SSH keys	24
	Organizing your devices	25
	View device information	25
	Refresh the devices	30
	View device summary reports	30
	View a system or device log	30
	Manage multiple devices	31
	Manage URL links for all devices	31
	Set up network traffic control on a device	32
	Configure SNMP notifications	33
	Sync device with ESM	33
	Set up communication with ELM	33
	Set default logging pool	34
	Grant access to your system	35
	Start, stop, reboot, or refresh a device	35
	Change connection with ESM	35

Virtual devices	36
Manage custom display types	40
Manage a group in a custom display type	40
Delete a group or device	41
Delete duplicate devices on the system navigation tree	41
Configuring devices	41
Event Receiver settings	42
Enterprise Log Search (ELS) settings	88
Enterprise Log Manager (ELM) settings	90
Advanced Correlation Engine (ACE) settings	111
Application Data Monitor (ADM) settings	117
Database Event Monitor (DEM) settings	133
Distributed ESM (DESM) settings	144
ePolicy Orchestrator settings	145
McAfee Vulnerability Manager settings	150
McAfee Network Security Manager settings	152
Configuring ancillary services	154
General system information	155
Configure Remedy server settings	155
Stop automatic refresh of ESM system tree	156
Defining message settings	156
Set up NTP on a device	158
Manage Global Blacklists page	160
Configure network settings	160
System time synchronization	175
Install a new certificate	176
Configure profiles	177
SNMP configuration	179
Managing the database	186
Set up database archival	186
Set up ESM data storage	187
Set up ESM VM data storage	188
Increase number of available accumulator indexes	188
Set up data retention limits	189
Define data allocation limits	189
Manage database index settings	190
Manage accumulator indexing	190
View database memory utilization	191
Working with users and groups	191
Add a user	192
Select user settings	193
Setting up security	194
Set up user credentials for McAfee ePO	200
Disable or re-enable a user	201
Authenticate users to an LDAP server	201
Set up user groups	202
Add a group with limited access	205
Backing up and restoring system settings	206
Back up ESM settings and system data	206
Restore ESM settings	208
Restore backed up configuration files	208
Work with backup files on ESM	209
Manage file maintenance	209
Setting up redundant ESMs	210
Set up ESM redundancy	210
Remove a redundant ESM	211

Enabling and disabling shared queries	211
Change redundant ESM to primary ESM	212
Managing the ESM	212
Manage logs	213
Mask IP addresses	215
Set up ESM logging	216
Regenerate SSH key	216
Queries task manager	217
Manage queries running on ESM	217
Update primary or redundant ESM	218
Using a global blacklist	218
Set up a global blacklist	219
Data enrichment	220
Add data enrichment sources	221
Add Hadoop HBase data enrichment source	224
Add Hadoop Pig data enrichment source	225
Add Active Directory data enrichment for user names	225
4 Working with dashboard views	227
Dashboard building blocks	227
Predefined (default) views	228
Open dashboard views	228
Add custom dashboard views	229
Bind dashboard widgets	229
Filter dashboard views	230
Respond to notifications	231
Investigate open cases	231
5 Managing cyber threats	233
Set up cyber threat management	233
Set up cyber threat feed for domain	234
View cyber threat feed results	235
Supported indicator types	235
Errors on manual upload of an IOC STIX XML file	236
6 Working with content packs	237
Importing content packs	237
Install content packs	237
Modify content packs	238
7 Alarms workflow	239
Prepare to build alarms	239
Set up alarm messages	239
Manage alarm audio files	244
Build alarms	244
Enable or disable alarm monitoring	245
Copy an alarm	245
Create alarms	246
Monitor and respond to alarms	250
View and manage triggered alarms	251
Manage alarm reports queue	252
Tune alarms	253
Create UCAPL alarms	254
Add health monitor event alarms	256
Add a Field Match alarm	263
Customize summary for triggered alarms and cases	265

	Add an alarm to rules	265
	Create SNMP traps as alarm actions	266
	Add a power failure notification alarm	266
	Manage out-of-sync data sources	267
8	Working with events	269
	Events, flows, and logs	269
	Set up events, flows, and logs downloads	270
	Limit time for data collection	271
	Define inactivity threshold settings	271
	Get events and flows	272
	Check for events, flows, and logs	273
	Define geolocation and ASN settings	274
	Aggregating events or flows	275
	Setting up event forwarding	278
	Managing reports	285
	Set start month for quarterly reports	285
	Add reports	286
	Add report layout	288
	Add an image component to a report	291
	Include an image in PDFs and reports	291
	Add a report condition	292
	Display host names in a report	292
	Description of <i>contains</i> and <i>regex</i> filters	293
	Working with ESM views	296
	Manage views	297
	View session details	297
	Filtering views	298
	Watchlists	301
	Flow views	306
	Enhanced ELM search view	307
	View components	308
	Working with the Query Wizard	311
	Custom type filters	317
	Create custom types	319
	Predefined custom types table	320
	Add Time custom types	320
	Name/value custom types	320
	Add name/value group custom type	321
	Add UCF and Windows event ID filters	321
	McAfee® Active Response searches	322
	Run an Active Response search	323
	Manage Active Response search results	323
	Add an Active Response data enrichment source	324
	Add an Active Response watchlist	325
9	Managing cases	327
	Add a case	327
	Create a case from an event	328
	Add events to an existing case	328
	Edit or close a case	330
	View case details	331
	Add case status levels	332
	Email cases	333
	View all cases	333
	Generate case management reports	334

10	Working with the Asset Manager	337
	How Asset Manager works	337
	Manage assets	338
	Define old assets	340
	Asset Sources	341
	Manage asset sources	341
	Manage vulnerability assessment sources	343
	Zone Management	343
	Manage zones	343
	Add a zone	344
	Export zone settings	345
	Import zone settings	345
	Add a subzone	347
	Asset, threat, and risk assessment	348
	Manage known threats	348
	Select data to view in Scorecard	349
11	Scorecard	351
	How Scorecard view works	351
	Select data to view in Scorecard	353
	View Policy Auditor data in Scorecard	353
	Configure Scorecard view	354
	Configure benchmark groups	354
12	Managing policies and rules	355
	Understanding the Policy Editor	355
	The Policy Tree	357
	Manage policies on the Policy Tree	357
	Set up rule and report for database audit trails	360
	Normalization	361
	Rule types and their properties	361
	ADM rules	362
	Advanced Syslog Parser (ASP) rules	378
	Correlation rules	387
	Data source rules	392
	DEM rules	394
	ESM rules	395
	Filter rules	396
	Add or edit a transaction tracking rule	397
	Variables	398
	Windows events rules	400
	Default Policy settings	401
	Set up Oversubscription Mode	401
	View policy update status for devices	401
	Rule operations	402
	Manage rules	402
	Import rules	402
	Import variables	404
	Export rules	404
	Filter existing rules	404
	View a rule's signature	406
	Retrieve rule updates	406
	Clear updated rule status	407
	Compare rule files	407
	View the rule change history	408
	Create a new watchlist of rules	408

Add rules to a watchlist	409
Assign tags to rules or assets	409
Modify aggregation settings	410
Override action on downloaded rules	411
Severity weights	412
Set the severity weights	412
View policy change history	413
Apply policy changes	413
Enable Copy Packet	414
A FIPS mode information	415
FIPS mode information	415
Check FIPS integrity	416
Adding a keyed device in FIPS mode	417
Back up and restore information for a device in FIPS mode	417
Enable communication with multiple ESM devices in FIPS mode	418
Troubleshooting FIPS mode	419
Index	421

Preface

This guide provides the information you need to work with your McAfee product.

Contents

- ▶ [About this guide](#)
- ▶ [Find product documentation](#)

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience





McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

Conventions

This guide uses these typographical conventions and icons.

<i>Italic</i>	Title of a book, chapter, or topic; a new term; emphasis
Bold	Text that is emphasized
Monospace	Commands and other text that the user types; a code sample; a displayed message
Narrow Bold	Words from the product interface like options, menus, buttons, and dialog boxes
Hypertext blue	A link to a topic or to an external website
	Note: Extra information to emphasize a point, remind the reader of something, or provide an alternative method
	Tip: Best practice information
	Caution: Important advice to protect your computer system, software installation, network, business, or data
	Warning: Critical advice to prevent bodily harm when using a hardware product

Find product documentation

On the **ServicePortal**, you can find information about a released product, including product documentation, technical articles, and more.

Task

- 1 Go to the **ServicePortal** at <https://support.mcafee.com> and click the **Knowledge Center** tab.
- 2 In the **Knowledge Base** pane under **Content Source**, click **Product Documentation**.
- 3 Select a product and version, then click **Search** to display a list of documents.

Tasks

- [Find localized information on page 10](#)
We provide localized (translated) McAfee ESM release notes, Help, product guide, and installation guide for:

Find localized information

We provide localized (translated) McAfee ESM release notes, Help, product guide, and installation guide for:

- Chinese, Simplified
- Chinese, Traditional
- English
- French
- German
- Japanese
- Korean
- Portuguese, Brazilian
- Spanish

Access localized online Help

Changing the language setting in ESM automatically changes the language used in the online Help.

- 1 Log on to ESM.
- 2 On the system navigation pane of the ESM console, select **Options**.
- 3 Select a language, then click **OK**.
- 4 Click the Help icon in the upper right corner of the ESM windows or select the **Help** menu. The Help displays in the language you selected.



If the Help appears in English only, localized Help is not yet available. A future update installs localized Help.

Find localized product documentation on the Knowledge Center

- 1 Visit the [Knowledge Center](#).
- 2 Search for localized product documentation using the following parameters:
 - Search terms — *product guide, installation guide, or release notes*
 - Product — McAfee Enterprise Security Manager
 - Version — Choose a release version
- 3 In the search results, click the relevant document title.
- 4 On the page with the PDF icon, scroll down until you see language links on the right side. Click the relevant language.
- 5 To open the localized version of the product document, click the PDF link.

1

Introduction

McAfee® Enterprise Security Manager (McAfee ESM) allows security and compliance professionals to collect, store, analyze, and act on events from a single location.

Contents

- ▶ *How McAfee® Enterprise Security Manager (McAfee ESM) works*
- ▶ *Devices and what they do*
- ▶ *Use ESM Help*
- ▶ *Find localized information*

How McAfee® Enterprise Security Manager (McAfee ESM) works

McAfee ESM collects and aggregates data and events from security devices, network infrastructures, systems, and applications. It then applies intelligence to that data, by combining it with contextual information about users, assets, vulnerabilities, and threats. It correlates that information to find incidents that are relevant. Using interactive, customizable dashboards, you can drill down on specific events to investigate incidents.

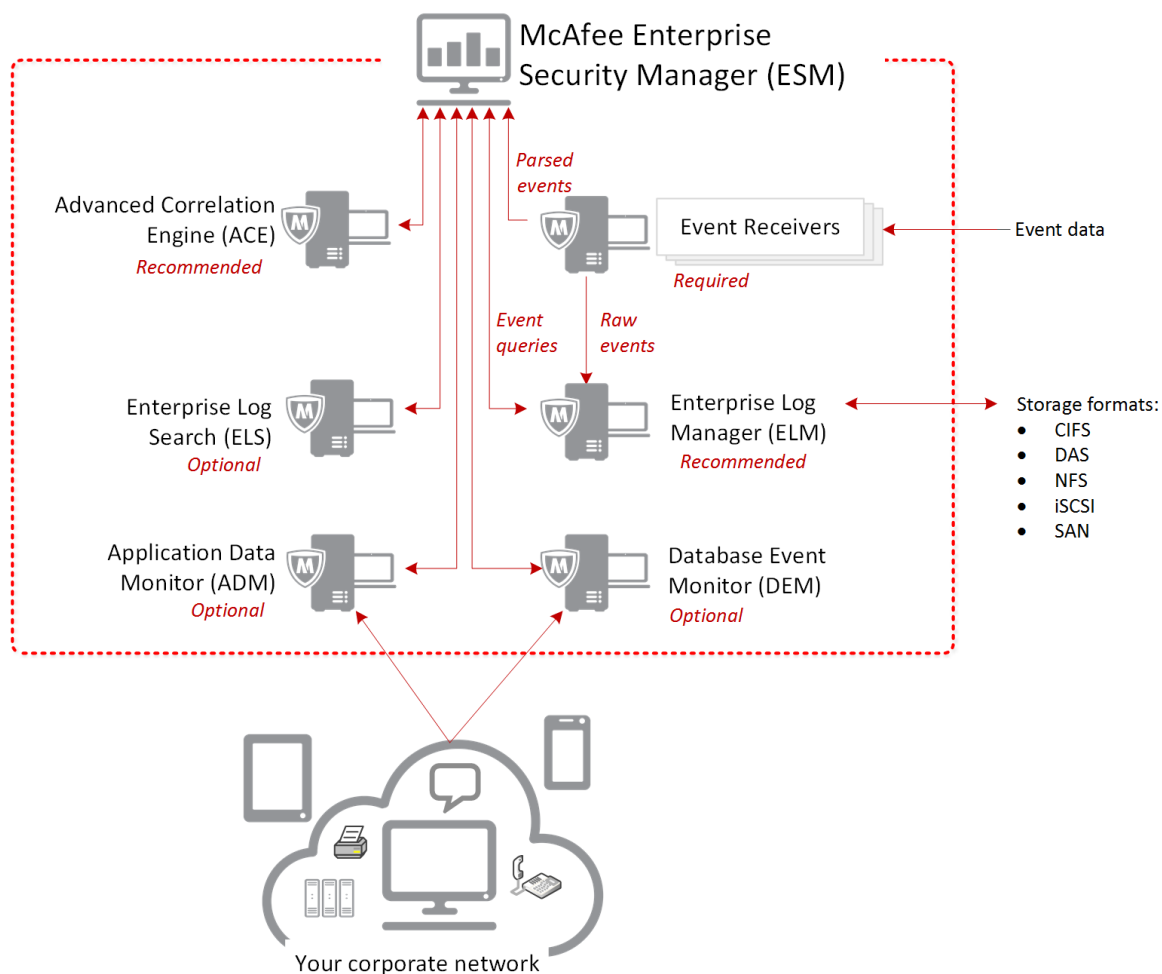
ESM is composed of three layers:

- **Interface** – A browser-based interface referred to as the *ESM console*.
- **Data storage, management, and analysis** – Devices that provide the storage, normalization, aggregation, configuration, reporting, visualization, and searching are:
 - ESM (required)
 - Advanced Correlation Engine (ACE) (highly recommended)
 - McAfee Enterprise Log Manager (ELM) (highly recommended)
 - Enterprise Log Search (ELS) (highly recommended)
- **Data collection** – Devices that provide the interfaces and services that acquire data from the user's network environment are:
 - Event Receiver (Receiver)
 - Application Data Monitor (ADM)
 - Database Event Monitor (DEM)

All command, control, and communication functions between the components are coordinated through secure communication channels.

Devices and what they do

The ESM enables you to administer, manage, and interact with all physical and virtual devices in your security environment. This diagram shows how ESM devices work together to collect and share data so that you can respond to potential threats in your environment.



See also

[Event Receiver settings on page 42](#)
[Enterprise Log Manager \(ELM\) settings on page 90](#)
[Application Data Monitor \(ADM\) settings on page 117](#)
[Database Event Monitor \(DEM\) settings on page 133](#)
[Advanced Correlation Engine \(ACE\) settings on page 111](#)
[Distributed ESM \(DESM\) settings on page 144](#)
[ePolicy Orchestrator settings on page 145](#)

Use ESM Help

Have questions about how to use ESM? Use the online Help as your context-sensitive information source, where you find conceptual information, reference materials, and step-by-step instructions on how to use ESM.

Task

- 1 To open ESM Help, do one of the following:
 - Select the menu option **Help | Help Contents**.
 - Click the question mark in the upper right of ESM screens to find context-sensitive Help specific to that screen.
- 2 From the Help window:
 - Use the **Search** field to find any word in the Help. Results appear below the Search field. Click the relevant link to display the Help topic in the pane on the right.
 - Use the **Contents** tab (table of contents) to view a sequential list of topics in the Help.
 - Use the **Index** to find a specific term in the Help. Keywords are organized alphabetically so you can scroll through the list until you find the keyword you want. Click the keyword to display that Help topic.
 - Print the current Help topic (without scroll bars) by clicking the printer icon in the upper right of the Help topic.
 - Find links to related Help topics by scrolling to the bottom of the Help topic.

Find localized information

We provide localized (translated) McAfee ESM release notes, Help, product guide, and installation guide for:

- Chinese, Simplified
- Chinese, Traditional
- English
- French
- German
- Japanese
- Korean
- Portuguese, Brazilian
- Spanish

Access localized online Help

Changing the language setting in ESM automatically changes the language used in the online Help.

- 1 Log on to ESM.
- 2 On the system navigation pane of the ESM console, select **Options**.

- 3 Select a language, then click **OK**.
- 4 Click the Help icon in the upper right corner of the ESM windows or select the **Help** menu. The Help displays in the language you selected.



If the Help appears in English only, localized Help is not yet available. A future update installs localized Help.

Find localized product documentation on the Knowledge Center

- 1 Visit the [Knowledge Center](#).
- 2 Search for localized product documentation using the following parameters:
 - Search terms — *product guide, installation guide, or release notes*
 - Product — McAfee Enterprise Security Manager
 - Version — Choose a release version
- 3 In the search results, click the relevant document title.
- 4 On the page with the PDF icon, scroll down until you see language links on the right side. Click the relevant language.
- 5 To open the localized version of the product document, click the PDF link.

2

Getting started

Verify that your ESM environment is current and ready to go.

Contents

- ▶ *Log on and off*
- ▶ *Customize the logon page*
- ▶ *Update ESM software*
- ▶ *Obtain and add rule update credentials*
- ▶ *Check for rule updates*
- ▶ *Change language for event logs*
- ▶ *Connecting devices*
- ▶ *Set console timeout value*

Log on and off

After you install and set up the devices, you can log on to the ESM console for the first time.

Task

- 1 Open a web browser on your client computer and go to the IP address that you set when you configured the network interface.
- 2 Type the default user name and password, then select the system language.
 - Default user name: `NGCP`
 - Default password: `security.4u`
- 3 Click **Log on** and read the **End User License Agreement**. Then click **Accept**.
- 4 Change your user name and password, then click **OK**.
- 5 Select whether to enable FIPS mode.



If FIPS mode is required, enable it the first time you log on to the system so that future operations with McAfee devices are in FIPS mode. Enable FIPS mode only when required because once enabled, it cannot be undone.

- 6 Follow the instructions to get your user name and password, which are needed for access to rule updates.
- 7 Perform initial ESM configuration:
 - a Select the language to be used for system logs.
 - b Select the time zone where this ESM is and the date format to be used with this account, then click **Next**.
 - c Define the settings using the **ESM Configuration** wizard pages.

- 8 Click **OK**.
- 9 When you complete your work session, log off using one of these methods:
 - If no pages are open, click **Sign out** from the drop-down list in the top-right corner of the page.
 - If pages are open, close the browser.

See also




[Customize the logon page on page 18](#)

[Change language for event logs on page 20](#)

Customize the logon page

Customize your login and print settings, edit system device links, and configure the settings for a remedy email server.

Task

- 1 To display **Custom Settings**, do one of the following:
 - From the dashboard, click  and select **System Properties | Custom Settings**.
 - From the system navigation tree, click  and select **Custom Settings**.
 - 2 Do any of the following:
 - To add custom text (such as company security policies) to your login screen, enter text in the box at the top of the page and select the **Include text on login screen** checkbox.
 - To add a custom image to your login screen, click **Select Image** and upload a specific image. Then select where you want the image to appear: on the login screen, on exported PDFs, on printed reports.
- 
- If you still see the old logo on the **Login** page after uploading a new custom logo, clear your browser cache.
- To delete an existing image, click **Delete Image**. The default logo is displayed. This option is available only if a custom image is uploaded.
 - Select whether to refresh the system tree automatically (every five minutes) and whether to refresh the system tree on update.
 - To change URL links for any system devices, click **Device Links**.
 - To configure Remedy e-mail server settings, click **Remedy**.
 - To set the starting month for quarterly reports and views, select the month from the drop-down button.

See also



[Log on and off on page 17](#)

[Change language for event logs on page 20](#)

Update ESM software

Access software updates from the updates server or from a security engineer, then upload them to ESM.

Task

- 1 To display **ESM Management**, do one of the following:
 - From the dashboard, click  and select **System Properties | ESM Management**.
 - From the system navigation tree, click  and select **ESM Management**.
- 2 Click the **Maintenance** tab, then click **Update ESM**.
- 3 Do one of the following:
 - Select the file you want to use to update your ESM, then click **OK**.
 - Browse to a software update file obtained from the McAfee ESM rules and updates server. Click **Upload**, then click **Yes** on the warning page.

ESM reboots and all current sessions are disconnected while the update is installed.

See also



[Obtain and add rule update credentials on page 19](#)

[Check for rule updates on page 20](#)

Obtain and add rule update credentials

McAfee ESM provides policy, parser, and rule updates as part of your maintenance contract. You have 30 days of access before your permanent credentials are required.

Task

- 1 Obtain your credentials by sending an email message to Licensing@McAfee.com with this information:
 - McAfee grant ID
 - Account name
 - Address
 - Contact name
 - Contact email address
- 2 When you receive your customer ID and password from McAfee, do one of the following:
 - From the dashboard, click  and select **System Properties | System Information | Rules Update**.
 - From the system navigation tree, click  and select **System Information | Rules Update**.
- 3 Click **Credentials**, then type the customer ID and password.
- 4 Click **Validate**.

See also



[Update ESM software on page 19](#)

[Check for rule updates on page 20](#)

Check for rule updates

McAfee continuously updates rule signatures used to examine network traffic. You can download rules updates automatically or manually from the McAfee server.

Task

- 1 Do one of the following:
 - From the dashboard, click  and select **System Properties | System Information**.
 - From the system navigation tree, click  and select **System Information**.
- 2 In **Rule Updates**, verify that your license is valid, then click **Rules Update**.
- 3 Select one of these options:
 - **Auto check interval** to set up the system to check for updates automatically with the frequency you select.
 - **Check Now** to check for updates now.
 - **Manual Update** to update the rules from a local file.
- 4 Click **OK**.

See also



[Update ESM software on page 19](#)

[Obtain and add rule update credentials on page 19](#)

Change language for event logs

When you first log on to ESM, you select the language for event logs, such as the health monitor log and device log. You can change this language setting.

Task

- 1 Do one of the following:
 - From the dashboard, click  and select **System Properties | ESM Management**.
 - From the system navigation tree, click  and select **ESM Management**.
- 2 Click **System Locale**, select a language from the drop-down list, then click **OK**.

See also

[Log on and off on page 17](#)

[Customize the logon page on page 18](#)

Connecting devices

To enable application and database monitoring, advanced rule- and risk-based correlation, and compliance reporting, connect both physical and virtual devices to McAfee ESM.

Contents

- [Add devices to the ESM console](#)
- [Select a display type](#)
- [Manage custom display types](#)

Add devices to the ESM console


After you set up and install the physical and virtual devices, add them to the ESM console.

Before you begin

Set up and install the devices.

Complete the following steps only for a complex ESM installation with multiple ESM devices. Do not complete this task for a simple ESM installation using a combination ESM.

Task

- 1 On the system navigation tree, click **Local ESM** or a group.
- 2 Click .
- 3 Select the type of device you are adding, then click **Next**.
- 4 In the **Device Name** field, enter a unique name in this group, then click **Next**.
- 5 Provide the information requested:
 - For McAfee ePO devices — Select a Receiver, type the credentials required to log on to the web interface, then click **Next**. To use for communicating with the database, type the settings.



Select **Require user authentication** to limit access to those users who have the user name and password for the device.

- For all other devices — Type the target IP address or URL for the device.
- 6 Select whether to use Network Time Protocol (NTP) settings on the device, then click **Next**.
 - 7 Enter a password for this device, then click **Next**.

ESM tests device communication and reports on the status of the connection.

See also

[Select a display type on page 21](#)

[Manage custom display types on page 22](#)

[Manage a group in a custom display type on page 40](#)

Select a display type

Select the way you want to display the devices in the system navigation tree.

Before you begin

Create custom display types.

Task

- 1 On the system navigation pane, click the drop-down arrow in the display type field.
- 2 Select one of the display types.

The device organization on the navigation tree changes to reflect the type you selected for the current work session.

See also

[Add devices to the ESM console on page 21](#)



[Manage custom display types on page 22](#)

[Manage a group in a custom display type on page 40](#)

Manage custom display types

Define how to organize devices on the system navigation tree using custom display types.

Task

- 1 On the system navigation pane, click the display type drop-down arrow.
- 2 Do one of the following:
 - To add custom display types, click **Add Display**, fill in the fields, then click **OK**.
 - To edit custom display types, click , change the settings, then click **OK**.
 - To delete custom display types, click  next to the display type you want to delete.

See also

[Add devices to the ESM console on page 21](#)



[Select a display type on page 21](#)

[Manage a group in a custom display type on page 40](#)

Set console timeout value

Define how long the current session on the ESM console can remain open without activity.

Task

- 1 Do one of the following:
 - From the dashboard, click  and select **System Properties | Login Security**.
 - From the system navigation tree, click  and select **Login Security**.
- 2 In **UI Timeout Value**, select the number of minutes that must pass without activity, then click **OK**.



If you select zero (0), the console stays open indefinitely.

3

Configuring McAfee ESM devices

McAfee ESM administers data, settings, updates, and communicates with multiple devices simultaneously. When creating McAfee ESM environment, carefully consider your organization's needs and compliance objectives to support your organization's security management life cycle.

Contents

- ▶ *About device keys*
- ▶ *Organizing your devices*
- ▶ *Configuring devices*
- ▶ *Configuring ancillary services*
- ▶ *Managing the database*
- ▶ *Working with users and groups*
- ▶ *Backing up and restoring system settings*
- ▶ *Setting up redundant ESMs*
- ▶ *Managing the ESM*
- ▶ *Using a global blacklist*
- ▶ *Data enrichment*

About device keys

For ESM to communicate with a device, it must encrypt all communications using the communications key that is created when the device is keyed.

All settings are stored on the ESM, which means that the ESM console is aware of the keys maintained on the ESM.

Device administrators can overwrite settings on the device from another ESM. Use a single ESM to manage devices attached to it. A DESM can handle the data collection from devices attached to another ESM.

Key a device

After you add a device to the ESM, you must key the device to enable communication. Keying the device adds security by ignoring all outside sources of communication.


Before you begin

If you are keying a distributed ESM after changing the IP address of the child, ensure that port 443 is open to reconnect with the ESM.



The following characters can't be used in a device name: ! @ # \$ % ^ & *) ([] { : ; ' ' > < , / ? ` ~ + = \ |

Task

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **ESM Management** and then select the **Key Management** tab.
If the device has an established connection and can communicate with the ESM, the **Key Device Wizard** opens.
- 3 Type a new password for the device, then click **Next**.
- 4 Click **Finish**.

See also

[Manage SSH keys on page 24](#)

Manage SSH keys

Devices can have SSH communication keys for systems they need to communicate with securely. You can stop communication with these systems by deleting the key.

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Key Management**, then click **Manage SSH Keys**.
The **Manage SSH Keys** page lists the IDs for the ESM that the device communicates with.
- 3 Highlight the ID and click **Delete** to stop communication with one of the systems listed.
- 4 Confirm the deletion, then click **OK**.

Table 3-1 Option definitions

Option	Definition
Authorized Keys table	View the machines this device has SSH communication keys for. If SSH is enabled, the machines on this list will communicate.
Known Hosts	For devices, manage the keys of any SSH-capable devices that this device has talked to (for example, Receiver to SCP data source). For the ESM, view the keys of all the devices in the system tree that the ESM talks to.
Known Hosts table	View IP address, device name, and fingerprint populated by host data available in the known_hosts file (root/.ssh/known_hosts).
Device's Fingerprint	View the fingerprint for this device, which is generated from the device's public SSH key.
Delete	Delete the selected item from the ESM.
View Key	View the key for the selected item.

See also

[Key a device on page 23](#)

Organizing your devices

The system navigation tree lists the devices on the system. You can select the way you want them displayed using the display type feature.

As you increase the number of devices on your system, it is helpful to organize them logically so you can find the ones you need to work with. For example, if you have offices in various locations, it might be best to display them by the zone they are in.

You can use the three predefined displays and you can design custom displays. Within each custom display, you can add groups to further organize the devices.

View device information

View general information about a device. Open the device's **Information** page to see the system ID, serial number, model, version, build, and more.

Task

For details about product features, usage, and best practices, click ? or Help.


- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 View the available information, then click **OK**.


Table 3-2 Option definitions

Option	Definition
Machine ID	Device identification number. To reactivate your system, McAfee Support asks for this number to send you the correct file.
Serial Number	Device serial number.
Model	Device model number.
Version	Software version currently running on the device
Build	Build number of the software version
Clock (GMT)	Date and time the device was last opened or refreshed
Sync Device Clock	Sync the clock on this device to the clock on the ESM.
Zone	Zone the device has been assigned to, if one has been assigned. If you click Zone , Zone Policy Manager opens (see <i>Add Zones</i>).
Policy	Current state of the policy on this device. If you click Policy , the Policy Editor opens (see <i>Policy Editor</i>).
Status	The status of the processes on the device and the FIPS status after running a FIPS self-test (if your device is running in FIPS mode).
Start	Starts the device. If the device is on, nothing occurs.
Stop	Stops the device. You are warned that all data collection stops.
Reboot	Restarts the device. You are warned that data collection stops for the time that the system is rebooting.
Refresh	Refreshes the information on the page

Table 3-3 Option definitions

Option	Definition
Device ID	Identification number assigned to the device. This number cannot be changed.
Name	Name you gave to the device when you added it to the system.
System Name	Name shown on the LCD or SSH display. It must begin with an alpha character and can only include alphanumeric characters and dashes.
URL	<p>Address where you can view event or flow details. It allows a maximum of 512 characters. If the URL address includes the address of a third-party application and you need to append variables representing data present in events or flows, click the variables icon and select the variable.</p> <p>To access the URL, click the Launch Device URL icon at the bottom of a table component for an event or flow view. It will take you to the third-party application, passing in the associated event or flow data via the URL.</p>
Description	Description of the device.

Tasks

- [Add URL link on page 27](#)
To view device information on a URL, you can set up the link on the **Name and Description** page for each device. When added, the link is accessible on the **Event Analysis** and **Flow Analysis** views for each device by clicking on the **Launch Device URL** icon  located at the bottom of the view components.
- [View device statistics on page 27](#)
View device-specific CPU, memory, queue, and other details for a device.
- [View message logs and device statistics on page 29](#)
You can view messages generated by the system, view statistics about the performance of the device, or download a .tgz file containing device status information.
- [Change the device name on page 29](#)
When you add a device to the system tree, you give it a name, which is displayed on the tree. This name, the system name, URL, and description, can be changed.

See also


[Add URL link on page 27](#)

[View device statistics on page 27](#)

[View message logs and device statistics on page 29](#)


[Change the device name on page 29](#)

Add URL link

To view device information on a URL, you can set up the link on the **Name and Description** page for each device. When added, the link is accessible on the **Event Analysis** and **Flow Analysis** views for each device by clicking on the **Launch Device URL** icon  located at the bottom of the view components.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Name and Description**, then type the URL.
- 3 Click **OK** to save the changes.

See also

[View device information on page 25](#)

[View device statistics on page 27](#)

[View message logs and device statistics on page 29](#)

[Change the device name on page 29](#)

View device statistics


View device-specific CPU, memory, queue, and other details for a device.

Before you begin

Verify that you have the Device Management permission.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the relevant device, then click the **Properties** icon .
- 2 Click device **Management**, then click **View Statistics**.

A graph displays statistics for that device and refreshes every 10 minutes. Displaying data requires a minimum of 30 minutes of data. Each metric type contains several metrics, some of them are enabled by default. Click **Displayed** to enable metrics. The fourth column indicates the scale of the corresponding metric.

Table 3-4 Option definitions

Option	Definition
Date Range	Select the time you want to view statistics for.
Metrics	Select the metric types that you want to view.
Refresh	Click to populate the graph and table with the statistics for the metrics you selected.
Graph	View the selected statistics in graph form.
Table	View the selected statistics in table form.
Group column	Lists the type of metric group.
Metric column	Lists the metrics, which are subcategories of the metric group.
Displayed column	Indicates the metrics that are currently shown in the graph. You can select or deselect the metrics and the graph reflects the changes.
Scale column	Indicates the scale of the corresponding metric.
Color column	Indicates the color of the line on the graph that represents each metric.

See also

[Add URL link on page 27](#)

[View device information on page 25](#)

[View message logs and device statistics on page 29](#)

[Change the device name on page 29](#)

[Performance monitor tab for device statistics on page 28](#)

Performance monitor tab for device statistics

View various statistics for the selected ESM or device.

Table 3-5 Option definitions

Option	Definition
Date Range	Select the time you want to view statistics for.
Metrics	Select the metric types that you want to view.
Refresh	Click to populate the graph and table with the statistics for the metrics you selected.
Graph	View the selected statistics in graph form.
Table	View the selected statistics in table form.
Group column	Lists the type of metric group.
Metric column	Lists the metrics, which are subcategories of the metric group.
Displayed column	Indicates the metrics that are currently shown in the graph. You can select or deselect the metrics and the graph reflects the changes.

Table 3-5 Option definitions *(continued)*

Option	Definition
Scale column	Indicates the scale of the corresponding metric.
Color column	Indicates the color of the line on the graph that represents each metric.

See also


[View device statistics on page 27](#)

View message logs and device statistics

You can view messages generated by the system, view statistics about the performance of the device, or download a .tgz file containing device status information.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click device **Management**, then select one of the following:

Option	Description
View Log	Click to view messages that were recorded by the system. Click Download Entire File to download the data to a file.
View Statistics	Click to view statistics about the performance of the device such as ethernet interface, ifconfig, and iptables filter.
Device Data	Click to download a .tgz file that contains data about the status of your device. You can use this when you are working with McAfee support to resolve an issue on your system.

See also

[Add URL link on page 27](#)

[View device statistics on page 27](#)

[View device information on page 25](#)


[Change the device name on page 29](#)

Change the device name

When you add a device to the system tree, you give it a name, which is displayed on the tree. This name, the system name, URL, and description, can be changed.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Name and Description**, then change the name, system name, URL, and description, or view the **Device ID** number.
- 3 Click **OK**.

See also

[Add URL link on page 27](#)

[View device statistics on page 27](#)

[View message logs and device statistics on page 29](#)

[View device information on page 25](#)

Refresh the devices

You can manually update the devices on the system so their information matches that on the ESM.

- On the actions toolbar, click the **Refresh Devices** icon .

View device summary reports

The device summary reports show the types and number of devices on the ESM and the last time an event was received by each one. These reports can be exported in comma-separated value (CSV) format.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **System Information** | **View Reports**.
- 2 View or export the **Device Type Count** or **Event Time** report.
- 3 Click **OK**.

Table 3-6 Option definitions

Option	Definition
Device Type Count	View a list of the types of devices and how many of each type are on the ESM.
Event Time	View the last time an event was received by each device on the ESM.
Export to CSV	Export a report in CSV format that contains this information to the location you specify.

View a system or device log

System and device logs show events that have taken place on the devices. You can view the summary page, which shows the event count and the times of the first and last event on ESM or device or view a detailed list of events on the **System Log** or **Device Log** page.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 View a summary of event data:
 - System data — On **System Properties**, click **System Log**.
 - Device data — On a device's **Properties** page, click **Device Log**.
- 2 To view the log of events, enter a time range, then click **View**.

The **System Log** or **Device Log** page lists all the events generated during the time range you specified.

Table 3-7 Option definitions

Option	Definition
Start Time, Stop Time	Change the time range for the list of events, then click Refresh .
Export	Click to export portions of or the whole log to a plain text file. You can export a maximum of 50,000 records at a time.
Filter icon in first (Status) column	Select if you want to view all, only status-related, or only non-status-related log events. Status-related log events are generated on the individual devices and are retrieved when events, flows, and logs are pulled from the device.
Filter icon in Category , Name , and Device Name columns.	Click to filter the events by their category, user name, or device.

Table 3-8 Option definitions

Option	Definition
Event Count	Total number of events that have been logged on the device.
First Event	Date and time that the first log event took place.
Last Event	Date and time that the last log event took place.
Start Time, Stop Time	If you want to view the events for a specific time range, enter the start and stop time in these fields.
View	Click to view the events for the time range you specified.

Manage multiple devices

The **Multi-Device Management** option allows you to start, stop, and restart, or update the software on multiple devices at one time.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 On the system navigation tree, select the devices you want to manage.
- 2 Click the **Multi-Device Management** icon  on the actions toolbar.
- 3 Select the operation you want to perform and the devices you want to perform it on, then click **Start**.

Table 3-9 Option definitions

Option	Definition
Operation	Select the operation you want to perform. <ul style="list-style-type: none">• Start — Starts the devices you select.• Stop — Stops the devices you select.• Reboot — Stops and restarts the devices you select.• Update — Updates the selected devices with the software you select on the Select Software Update File page.
Device Name	View a list of the devices that can be managed.
Include column	Select the devices.
Select All	Click to select all devices.
Select None	Click to deselect all devices.
Start	Click to begin the operation.
Status column	View the status of the operation for each device.
Close	Click to close the Multi-Device Management page. The operation continues until it is completed.

Manage URL links for all devices

You can set up a link for each device to view device information on a URL.

Before you begin

Set up the URL site for the device.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Custom Settings | Device Links**.
- 2 To add or edit a URL, highlight the device, click **Edit**, then enter the URL.
The URL field has a limit of 512 characters.
- 3 Click **OK**.

You can access the URL by clicking the **Launch Device URL** icon  at the bottom of the **Event Analysis** and **Flow Analysis** views for each device.

Table 3-10 Option definitions

Option	Definition
Device Name column	Lists all the devices on the ESM.
URL column	Shows the URL addresses already set up for each device.
Edit	Opens the Edit URL page where you can type the URL address.
Remove URL	Deletes the URL for the selected device.

Table 3-11 Option definitions

Option	Definition
URL	Type the address for the URL site for this device.
Variable icon	If the URL address you entered includes the address of a third-party application and you need to append variables to the URL address representing data present in events and flows, click the location in the URL address where the variable must be inserted, then click the variable icon and select the variable.

Set up network traffic control on a device

Define a maximum data output value for Receiver, ACE, ELM, ADM, and DEM devices.


This feature is helpful when you have bandwidth restrictions and must control the amount of data that each of these devices can send out. The options are kilobits (Kb), megabits (Mb), and gigabits (Gb) per second.



Be careful when configuring this feature because limiting traffic might result in data loss.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the device, then click the **Properties** icon .
- 2 Click the **Configuration** option for the device, click **Interfaces**, then click the **Traffic** tab.
The table lists the existing controls.
- 3 To add controls for a device, click **Add**, enter the network address and mask, set the rate, then click **OK**.

If you set the mask to zero (0), all data sent is controlled.
- 4 Click **Apply**.

The outbound traffic speed of the network address you specified is controlled.

Table 3-12 Option definitions

Option	Definition
Network column	Displays the addresses of the networks where the system controls outbound traffic, based on what you have defined.
Mask column	Displays the masks for the network addresses.
Maximum Throughput column	Displays the maximum throughput you defined for each network.
Add, Edit, Delete	Manage the network addresses that you want to control.

Table 3-13 Option definitions

Option	Definition
Network	Type the address of the network where you want to control outbound traffic on.
Mask	Select a mask for the network address. Select 0 for ALL.
Rate	Select kilobits (Kb), megabits (Mb), or gigabits (Gb), then select the rate per second for sending traffic.

See also

[Add throughput rate page on page 171](#)

Configure SNMP notifications


To configure device-generated SNMP notifications, you must define which traps to send and their destinations.



If you are setting up SNMP on an HA Receiver, the traps for the primary Receiver go out through the shared IP address. Therefore, when you set up the listeners, you need to set one up for the shared IP address.

Task


For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Configuration | SNMP**.
- 3 Define the settings, then click **OK**.

Sync device with ESM

If you have to replace an ESM, sync it to restore the settings. If you don't have a current database backup, you must also sync the data source, virtual device, and database server settings with ESM so they can resume pulling events.

Task


- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **<device label> Configuration | Sync Device**.
- 3 When the sync is completed, click **OK**.

Set up communication with ELM

If you are sending the data from this device to the ELM, **ELM IP** and **SYNC ELM** appear on the device's **Configuration** page, allowing you to update the IP address and sync the ELM with the device.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Configuration**, then do one of the following:

Click...	To do this...
ELM IP	Update the IP address for the ELM to which this device is linked. You must do this if you change the IP address for the ELM or if you change the ELM management interface through which this device communicates with the ELM.
Sync ELM	Sync the ELM with the device if one of them has been replaced. When you use this feature, the SSH communication between the two devices is re-established, using the key for the new device with the previous settings.

Set default logging pool


If you have an ELM device on your system, you can set up a device so the event data it receives is sent to the ELM device. To do this, you must configure the default logging pool.



The device does not send an event to the ELM until after its aggregation time period has expired.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Configuration | Logging**.
- 3 Make the appropriate selections on the pages that open.

You are informed when logging of data from this device to the ELM is enabled.

Table 3-14 Option definitions

Option	Definition
Log Configuration page	Select Logging to enable it.
Logging link	Click to access ELM Logging Options page.
ELM Logging Options page	Select the storage pool on the ELM that you want the data logged on.
Device - ELM Association page	If you haven't selected the ELM you want to log the data on, confirm that you want to do this. Once this association is made, it can't be changed.
Select ELM for Logging page	If you have more than one ELM on the system, select the one you want the data logged on.
Select ELM IP Address page	Select the IP address you want the device to communicate with the ELM through.
No ELM Pools page	If you don't have any storage pools on the ELM, go to ELM Properties Storage Pools to add them.

See also


[Receiver data sources on page 52](#)

Grant access to your system

When you place a support call to McAfee, you might need to grant access so the technical support engineer can see your system.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click device **Management | Connect**.

The button changes to **Disconnect** and your IP address is provided.

- 3 Give the IP address to the technical support engineer.



You might need to provide additional information, such as the password.


- 4 Click **Disconnect** to end the connection.

Start, stop, reboot, or refresh a device

Start, stop, reboot, or refresh a device on the **Information** page.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Verify that device **Information** is selected, then click **Start, Stop, Reboot, or Refresh**.

Change connection with ESM

When you add a device to the ESM, you set up its connection with the ESM. You can change the IP address and port, disable SSH communication, and check the status of the connection.

Before you begin

If you are keying a distributed ESM after changing the IP address of the child, ensure that port 443 is open to reconnect with the ESM.



Changing these settings doesn't affect the device itself. It only affects the way the ESM communicates with the device.

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Connection**, then make the changes.
- 3 Click **Apply**.

Table 3-15 Option definitions

Option	Definition
Target IP Address/Name	Type the IP address or host name the ESM uses to communicate with the device.
Target Port	Select the port used to attempt communication (default port is 22).
Device ID	View the identification number for the device.
Mark this device as disabled	Select to stop SSH communication to the ESM. The icon for this device on the system navigation tree will indicate it is disabled.
Status	(Optional) Click to check the connection.

Table 3-16 Option definitions

Option	Definition
Associated Receiver	Select the Receiver associated with the device. You can select the link to open the Receiver's Properties page.
Database login parameters	Change the database login parameters so you can pull events.
Website UI credentials	Change the settings to access the Web user interface.
Require user authentication	Select to require all users to authenticate with a user name and password prior to accessing the device.
Connect	Click either of them to test the connection to the database or to the web.

Virtual devices

You can add virtual devices to some ADM device models to monitor traffic, compare traffic patterns, and for reporting.

Purpose and benefits

Virtual devices can be used for several purposes:

- Compare traffic patterns against rule sets. For example, you can set up a virtual device that only looks at web traffic ports and set up a policy where you can enable or disable different rules.
- Reporting. Using it in this manner is like having an automatic filter set up.
- Monitor multiple paths of traffic at once. By using a virtual device, you can have separate policies for each path of traffic and sort different traffic into different policies.

Maximum number of devices per model

The number of virtual devices that can be added to an ADM is based on the model:

Device maximum	Model
2	APM-1225 APM-1250
4	APM-2230 APM-3450
0	APM-VM

How selection rules are used

Selection rules are used as filters to determine the packets that a virtual device processes.

For a packet to match a selection rule, all filter criteria defined by that rule must be matched. If the packet's information matches all filter criteria for a single selection rule, the virtual device that contains the matching selection rule processes it. Otherwise, it is passed on to the next virtual device in order. The ADM itself then processes it, as a default, if no selection rules are matched on any virtual devices.

Things to note for IPv4 virtual devices:

- All packets for a single connection are sorted based only on the first packet in the connection. If the first packet in a connection matches a selection rule for the third virtual device in the list, all subsequent packets in that connection go to the third virtual device. This happens even if the packets match a virtual device that is higher in the list.
- Invalid packets (a packet that is not setting up a connection or part of an established connection) are sorted to the base device. For example, you have a virtual device that is looking for packets with a source or destination port of 80. When an invalid packet comes through with a port of 80, it is sorted to the base device instead of the virtual device that looks for port 80 traffic. So, you see events in the base device that look like they should have gone to a virtual device.

The order that selection rules are listed is important because the first time a packet matches a rule, that packet is automatically routed to that virtual device for processing. For example, you add four selection rules and the fourth one in order is the filter that triggers most often. This means each packet must pass over the other filters for this virtual device before getting to the most commonly triggered selection rule. To enhance the efficiency of the processing, make the most commonly triggered filter first in order, instead of last.

Order of virtual devices

The packets coming into the ADM device are compared to the selection rules for each virtual device in the order that the virtual devices are set up. So, order in which virtual devices are checked is important. The packet makes it to the selection rules for the second virtual device only if it doesn't match any selection rules on the first device.

To change the order on an ADM device, go to **Edit Virtual Device** page (**ADM Properties** | **Virtual Devices** | **Edit**) and use the arrows to put them in the correct order.

ADM virtual devices

ADM virtual devices monitor traffic on an interface. There can be up to four ADM interface filters on your system. Each filter can be applied to only one ADM virtual device at a time. If a filter is assigned to an ADM virtual device, it does not appear on the list of available filters until it is removed from that device.

Invalid packets (a packet that is not setting up a connection or part of an established connection) are sorted to the base device. For example, if an ADM virtual device is looking for packets with a port of 80, and an invalid packet comes through with a port of 80, it is sorted to the base device. So, you can see events in the base device that look like they should have gone to an ADM virtual device.

See also[Add a virtual device on page 38](#)[Manage selection rules on page 38](#)**Manage selection rules**

Selection rules are used as filters to determine which packets are processed by a virtual device. You can add, edit, and delete selection rules.

The order the rules are listed in is important because the first time a packet matches a rule, that packet is routed to that virtual device for processing.

Task

For details about product features, usage, and best practices, click ? or **Help**.


1 Select an ADM device, then click the **Properties** icon .

2 Click **Virtual Devices**, then click **Add**.

The **Add Virtual Device** window opens.

3 Add, edit, remove, or change the order of the selection rules in the table.

Table 3-17 Option definitions

Option	Definition
ADM Add Selection Rule page	Select one of the interface filters, then click OK .
	 There can be up to four ADM interface filters. Each filter can only be applied to one ADM virtual device at a time.

See also[Virtual devices on page 36](#)**Add a virtual device**

You can add a virtual device to some ADM devices, setting the selection rules that determine which packets each device processes.

Before you begin

Make sure that virtual devices can be added to the device you have selected (see *About virtual devices*).

Task

For details about product features, usage, and best practices, click ? or **Help**.

1 On the system navigation tree, select an ADM device, then click the **Properties** icon .


2 Click **Virtual Devices** | **Add**.

- 3 Enter the information requested, then click **OK**.
- 4 Click **Write** to add the settings to the device.

Table 3-18 Option definitions

Option	Definition
Virtual Devices table	Lists the virtual devices currently on the ADM.
Logging	Activates or deactivates logging on all the virtual devices.
Set a storage pool... icon	Opens ELM Logging Options page so you can add a storage pool to the selected virtual devices.
Add	Opens the Add Virtual Device page.
Edit	Opens the Edit Virtual Device page, where you can change the settings for the selected virtual device.
Remove	Deletes the selected device from the table.
Move Up and Move Down arrows	Moves the selected virtual device up or down in the list of devices on the system. Their order is important because packets are processed starting with the first virtual device on the list, and working down from there.
Write	Writes any changes made to the virtual devices to the ADM.

Table 3-19 Option definitions

Option	Definition
Name	Type a name for the virtual device.
URL	Enter the URL address where you can view this virtual device's information, if you have one set up. Click the Variables icon  if you need to add a variable to the address.
Enabled	Select if you want the device enabled.
Storage Pool	If you have an ELM on your system and you want data that is received by this device to be logged on the ELM, click this link, then select the storage pool.
Zone	If zones are defined on your system (see <i>Zone Management</i>), select the zone this virtual device must be assigned to.
Description	Add notes or important information about the device.
Add	Click to add selection rules to the device, which determines which packets it processes.
Edit	Click to change the settings on the Selection Rule .
Remove	Click to delete the selected rule.
Move Up and Move Down arrows	Change the order of the rules.



See also

[Virtual devices](#) on page 36

Manage custom display types

Define how to organize devices on the system navigation tree using custom display types.

Task

- 1 On the system navigation pane, click the display type drop-down arrow.
- 2 Do one of the following:
 - To add custom display types, click **Add Display**, fill in the fields, then click **OK**.
 - To edit custom display types, click , change the settings, then click **OK**.
 - To delete custom display types, click  next to the display type you want to delete.

See also

[Add devices to the ESM console on page 21](#)

[Select a display type on page 21](#)

[Manage a group in a custom display type on page 40](#)

Manage a group in a custom display type

You can use groups in a custom display type to organize your devices into logical groupings.





Before you begin

Add a custom display type (see *Manage custom display types*).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation pane, click the display type drop-down list.
- 2 Select the custom display, then do one of the following:

To...	Do this...
Add a new group	<ol style="list-style-type: none"> 1 Click a system or group node, then click the Add Group icon  on the actions toolbar. 2 Fill in the fields, then click OK. 3 Drag-and-drop devices on the display to add them to the group. <div>  If the device is part of a tree on the display, a duplicate device node is created. You can then delete the duplicate on the system tree. </div>
Edit a group	Select the group, click the Properties icon  , then make changes on the Group Properties page.
Delete a group	Select the group, then click the Delete Group icon  . The group and the devices that are in it are deleted from the custom display. The devices are not deleted from the system.

See also

[Add devices to the ESM console on page 21](#)

[Select a display type on page 21](#)

[Manage custom display types on page 22](#)

Delete a group or device

When a device is no longer part of the system or you no longer use a group, delete it from the system navigation tree.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 On the system navigation tree, highlight the device or group that you want to delete, then click the **Delete** icon on the actions toolbar.
- 2 When prompted to confirm, click **OK**.

Delete duplicate devices on the system navigation tree

Duplicate device nodes can appear on the system navigation tree when you drag and drop devices from a system tree into a group or when you have groups set up and then upgrade the ESM software. We recommend that you delete them to avoid confusion.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation pane, click the display type drop-down list.
- 2 Select the **Edit** icon  next to the display that includes the duplicate devices.
- 3 Deselect the duplicate devices, then click **OK**.

The devices that had duplicates are now listed only in their assigned groups.

Configuring devices

To enable real-time forensics, application and database monitoring, advanced rule- and risk-based correlation, and compliance reporting, connect both physical and virtual devices to McAfee ESM .

Table 3-20 Option definitions

Option	Definition
ACL Settings	Set up access control settings to limit access to the device.
Advanced DEM settings	Define settings for DEM logs.
Apply	Click to write the configuration settings to the DEM.
Compression	Set the level of compression to be applied to all data coming in to the ELM.
Data	Select the type of data to be sent from the ESM to the device.
Data Archival	Set up the Receiver to forward a backup of the raw data to your storage device for long-term storage.
ELM IP	If you have chosen to send the data from this device to the ELM, you can update the IP address for the ELM this device is linked to.
Flow	Enable or disable logging of flow data.
Interface	Set up the network interfaces for the device with the ESM.
License	View and update the DEM license information.
Logging	If you have an ELM device on your system, set the default logging pool for the device if you want the data received to be sent to the ELM.

Table 3-20 Option definitions *(continued)*

Option	Definition
Migrate DB	On an ELM device, set up an alternate location to store records it generates.
Network Time Protocol (NTP) Settings	Synchronize the device's time with an NTP server.
Passwords	If the rule for the event whose session data you are viewing is password-related, select if you want the password related to the event to be displayed on the Session Viewer .
Restore Config	Restore the configuration file for this device, which was saved during the ESM backup process. This backup includes SSH, Network, SNMP, and other .conf files.
SNMP Traps	Configure the SNMP traps generated by the device.
Sync Device	Sync the device data source or virtual device settings with those on the ESM. If you are syncing a Receiver, the dependent devices on the Receiver are also added as devices to the McAfee ESM.
Sync ELM	If you have chosen to send the data from this device to the ELM, sync the ELM with the device.
Sync Files	Click to sync all DEM configuration files.
Time Zone	Set the ADM to your time zone.

Contents

- [Event Receiver settings](#)
- [Enterprise Log Search \(ELS\) settings](#)
- [Enterprise Log Manager \(ELM\) settings](#)
- [Advanced Correlation Engine \(ACE\) settings](#)
- [Application Data Monitor \(ADM\) settings](#)
- [Database Event Monitor \(DEM\) settings](#)
- [Distributed ESM \(DESM\) settings](#)
- [ePolicy Orchestrator settings](#)
- [McAfee Vulnerability Manager settings](#)
- [McAfee Network Security Manager settings](#)

Event Receiver settings

The **Event Receiver** enables the collection of security events and network flow data from multi-vendor sources including firewalls, virtual private networks (VPNs), routers, NetFlow, sFlow, and others.

The **Event Receiver** allows for the collection of this data and normalizes it into a single manageable solution. This provides you with a single view across devices from multiple vendors, such as Cisco, Check Point, and Juniper, and allows event and flow data collection.

High availability Receivers (Receiver-HA) can be used in primary and secondary mode, acting as backups for each other. The secondary Receiver (B) monitors the primary Receiver (A) continuously and new configuration or policy information is sent to both devices. When Receiver B determines that Receiver A failed, it disconnects Receiver A's data source NIC from the network and takes over as the new primary. It remains as the primary until you intervene manually to restore Receiver A as primary.

See also

[View streaming events on page 43](#)

[High Availability Receivers on page 43](#)

[Archiving Receiver raw data on page 50](#)

View streaming events

The **Streaming Viewer** displays a list of events as they are generated by McAfee ePO, McAfee® Network Security Manager, Receiver, data source, child data source, or the client you select. You can filter the list and select an event to display in a view.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 On the system navigation tree, select the device you need to view, then click the **View Streaming Events** icon  in the actions toolbar.
- 2 Click **Start** to begin streaming and **Stop** to stop it.
- 3 Select any of the available actions on the viewer.
- 4 Click **Close**.

Table 3-21 Option definitions

Option	Definition
Start	Start the streaming.
Stop	Stop the streaming.
Table	View the events as they come in to the device.
Packet section	View the details for the event you select.
Filters icon	To filter the events as they are generated, click and enter the information you want to filter. Only those events that match the filters are displayed.
Columns icon	Change the columns that are displayed in the streaming table.
Clear All icon	Clear the current list of events.
Launch View icon	View the selected event in a view. To see it, close the viewer. The event is displayed in the views section of the console.

See also

[Event Receiver settings on page 42](#)

High Availability Receivers

High Availability Receivers are used in primary and secondary mode so that the secondary Receiver can swiftly take over functions when the primary Receiver fails. This provides continuity of data collection that is better than that provided by a single Receiver.



The High Availability Receivers feature is not FIPS-compliant. If you are required to comply with FIPS regulations, do not use this feature.

This setup consists of two Receivers, one acting as the primary or preferred primary and the other as secondary. The secondary Receiver monitors the primary continuously. When the secondary determines that the primary has failed, it stops the primary and takes over its function.

Once the primary is repaired, it becomes the secondary or it becomes the primary once again. This is determined by the option selected in the **Preferred primary device** field on the **HA Receiver** tab (see *Set up Receiver-HA Devices*).

These Receiver models can be purchased with High Availability function:

- ERC-1225-HA
- ERC-2230-HA
- ERC-2250-HA
- ERC-4245-HA
- ERC-4500-HA
- ERC-1250-HA
- ERC-1260-HA
- ERC-2600-HA
- ERC-4600-HA

These models include an Intelligent Platform Management Interface (IPMI) port as well as at least 4 NICs, which are necessary for HA functionality (see *Network ports on Receiver-HA*).

The IPMI cards eliminate the possibility of both DS NICs using the shared IP and MAC at the same time by shutting down the failed receiver. The IPMI cards are connected with a cross-over or straight-through cable to the other Receiver. The Receivers are connected with a cross-over or straight-through cable on the heartbeat NIC. There is a management NIC for communication with the ESM, and a data source NIC for collecting data.

When the primary Receiver is running properly and the secondary Receiver is in secondary mode, this is happening:

- The Receivers communicate constantly over the dedicated heartbeat NIC and the management NIC.
- Any certificates that are received, such as OPSEC or Estreamer, are passed to the other Receiver in the pair.
- All data sources use the data source NIC.
- Each Receiver monitors and reports its own health. This includes internal health items like disk errors, database freezes, and lost links on NICs.
- The ESM communicates with the receivers periodically to determine their status and health.
- Any new configuration information is sent to both the primary and secondary receiver.
- The ESM sends policy to both the primary and secondary receiver.
- Stop/Reboot/Call Home apply to each receiver independently.

The following sections describe what happens when Receiver-HA experiences problems.

Primary Receiver failure

Determination of primary Receiver failure is the responsibility of the secondary receiver. It must determine that failure quickly and accurately to minimize data loss. On fail-over, all data since the primary last sent data to the ESM and ELM is lost. The amount of data lost depends on the throughput of the Receiver and the rate at which the ESM pulls data from the Receiver. These competing processes must be carefully balanced to optimize data availability.

When the primary Receiver fails completely (power loss, CPU failure) there is no heartbeat communication with the primary Receiver. Corosync recognizes the loss of communication and marks the primary Receiver as failed. Pacemaker on the secondary Receiver requests that the IPMI card on the primary Receiver shut down the primary Receiver. The secondary Receiver then assumes the shared IP and MAC address, and starts all collectors.

Secondary Receiver failure

The secondary failure process occurs when the secondary Receiver is no longer responding to the heartbeat communication. This means the system has been unable to communicate with the secondary Receiver after attempting to do so for a period of time using the management and heartbeat interfaces.

If the primary is unable to get heartbeat and integrity signals, corosync marks the secondary as failed and pacemaker uses the secondary's IPMI card to shut it down.

Primary health problem

The health of the primary receiver can be severely compromised. Severely compromised health would include a non-responsive database, an unresponsive data source interface, and excessive disk errors.

When the primary Receiver notices a healthmon alert for any of these conditions, it kills the corosync and pacemaker processes and sets a healthmon alert. Killing these processes causes the data collection duties to transfer to the secondary Receiver.

Secondary health problem

When the health of the secondary Receiver is severely compromised, this occurs:

- The secondary Receiver reports health problems to the ESM when queried and kills the corosync and pacemaker processes.
- If the secondary Receiver is still part of the cluster, it removes itself from the cluster and is unavailable in case of primary Receiver failure.
- The health problem is analyzed and a repair attempted.
- If the health problem is resolved, the Receiver is returned to normal operation using the *Return to service* procedure.
- If the health problem is not resolved, the *Replace a failed Receiver* process is initiated.

Returning to service

When a Receiver is returned to service after a failure (for example, restart after a power failure, hardware repair, or network repair), the following occurs:

- Receivers in High Availability mode do not start collecting data on startup. They are in secondary mode until they are set as primary.
- The preferred primary device assumes the role of primary and starts using the shared data source IP to collect data. If there is no preferred primary device, the device that is currently primary starts using the shared data source and collects data.

For details regarding this process, see *Replace a failed Receiver*.

Upgrading Receiver-HA

The Receiver-HA upgrade process upgrades both receivers sequentially, starting with the secondary receiver. It occurs like this:

- 1 The upgrade tarball file is uploaded to the ESM and applied to the secondary Receiver.
- 2 You switch the role of the primary and secondary Receiver, using the *Switch Receiver-HA roles* process, so the Receiver that was upgraded is now the primary Receiver and the one that has not yet been upgraded is secondary.
- 3 The upgrade tarball is applied to the new secondary receiver.
- 4 You once again switch the role of the primary and secondary Receiver, using the *Switch Receiver-HA roles* process, so the original Receiver roles are assumed once again.

When upgrading, it is best not to have a preferred primary Receiver. Refer to

If your Receiver-HA is set up with a preferred primary, it is best to change the setting before upgrading. On the **HA Receiver** tab (see *Set up Receiver-HA Devices*), select **None** in the **Preferred primary device** field. This allows you to use the **Fail-over** option, which is not available with a preferred primary setting. After both Receivers are upgraded, you can apply the preferred primary setting again.

See also

[Event Receiver settings](#) on page 42

[Set up Receiver-HA Devices](#) on page 46

[Reinitialize the secondary device](#) on page 46

[Set up Receiver HA with IPv6](#) on page 47

[Reset HA devices](#) on page 48

[Switch Receiver-HA roles](#) on page 49

[Replace a failed Receiver](#) on page 49

[Troubleshooting failed Receiver](#) on page 50

Set up Receiver-HA Devices

Define the settings for the Receiver-HA devices.

Before you begin


Add the Receiver that serves as the primary device (see *Add devices to the ESM console*). It must have three or more NICs.



The High Availability Receivers feature is not FIPS-compliant. If you are required to comply with FIPS regulations, do not use this feature.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the Receiver that will be the primary HA device, then click the **Properties** icon .
- 2 Click **Receiver Configuration**, then click **Interface**.
- 3 Click the **HA Receiver** tab, then select **Setup High Availability**.
- 4 Fill in the information requested, then click **OK**.

This initiates the process that keys the second Receiver, updates the database, applies `globals.conf`, and syncs the two Receivers.

See also

[High Availability Receivers](#) on page 43

[Reinitialize the secondary device](#) on page 46

[Set up Receiver HA with IPv6](#) on page 47

[Reset HA devices](#) on page 48

[Switch Receiver-HA roles](#) on page 49

[Replace a failed Receiver](#) on page 49

[Troubleshooting failed Receiver](#) on page 50

Reinitialize the secondary device

If the secondary Receiver is taken out of service for any reason, reinitialize it once it's reinstalled.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **Receiver Properties** for the primary Receiver, then click **Receiver Configuration** | **Interface** | **HA Receiver**.
- 2 Verify that the correct IP address is in the **Secondary Management IP** field.
- 3 Click **Reinitialize Secondary**.

The ESM performs the necessary steps to reinitialize the Receiver.

See also

[High Availability Receivers on page 43](#)

[Set up Receiver-HA Devices on page 46](#)

[Set up Receiver HA with IPv6 on page 47](#)

[Reset HA devices on page 48](#)

[Switch Receiver-HA roles on page 49](#)

[Replace a failed Receiver on page 49](#)

[Troubleshooting failed Receiver on page 50](#)

Set up Receiver HA with IPv6

Follow this process to set up high availability with IPV6 because you can't set the IPV6 address manually using the LCD.

Before you begin

- Ensure that the ESM is using IPv6, either manual or auto (**System Properties** | **Network settings**).
- Know the shared IP address, which the network administrator creates.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the two Receivers in the HA pair:
 - a Turn on the Receiver, then enable IPv6 using the LCD.
 - b Navigate to **Mgt IP Configr** | **Mgt1** | **IPv6**, and write down the management IP address. This might take some time due to network latency.
- 2 Add one of these Receivers to the ESM (see *Add devices to the ESM console*).
 - **Name** — Name of the HA pair.
 - **Target IP Address or URL** — Management IPv6 address for this HA Receiver, which you wrote down.
- 3 Select the newly added device on the system navigation tree, then click **Receiver Properties** | **Receiver Configuration** | **Interface**.
- 4 In the **IPv6 Mode** field, select **Manual** (the only supported mode for HA).
- 5 Click **Setup** next to the number 1 interface, type the shared IP address in the **IPv6** field, then click **OK**.

This address is assigned to the shared interface during HA setup. If this isn't done, HA doesn't fail over properly.

- 6 On **Receiver Properties**, click **Connection**, enter the shared IPv6 address in **Target IP Address/Name**, then click **OK**.
- 7 Continue with the HA setup process presented in *Set Up Receiver-HA devices*.

See also

High Availability Receivers on page 43
Set up Receiver-HA Devices on page 46
Reinitialize the secondary device on page 46
Reset HA devices on page 48
Switch Receiver-HA roles on page 49
Replace a failed Receiver on page 49
Troubleshooting failed Receiver on page 50

Reset HA devices

If you need to reset HA Receivers to the state they were in before being set up as HA devices, you can do so on the ESM console or, if communication with the Receivers fails, on the LCD menu.

- Do one of the following:

To...	Do this...
Reset a Receiver on the ESM console	<ol style="list-style-type: none"> 1 On the system navigation tree, click Receiver Properties, then click Receiver Configuration Interface. 2 Deselect Setup High Availability, then click OK. 3 Click Yes on the warning page, then click Close. <p>Both Receivers restart after a timeout of about five minutes, returning the MAC addresses to their original values.</p>
Reset the primary or secondary Receiver on the LCD menu	<ol style="list-style-type: none"> 1 On the Receiver's LCD menu, press X. 2 Press the down arrow until you see Disable HA. 3 Press the right arrow once to display Disable Primary on the LCD screen. 4 To reset the primary Receiver, press the checkmark. 5 To reset the secondary Receiver, press the down arrow once, then press the checkmark.

See also

High Availability Receivers on page 43
Set up Receiver-HA Devices on page 46
Reinitialize the secondary device on page 46
Set up Receiver HA with IPv6 on page 47
Switch Receiver-HA roles on page 49
Replace a failed Receiver on page 49
Troubleshooting failed Receiver on page 50

Switch Receiver-HA roles


The user-initiated switch-over process allows you to switch the roles of the primary and secondary Receivers. You might need to do this when upgrading a Receiver, preparing a Receiver to be returned to the manufacturer, or moving cables on a Receiver. This switch minimizes the amount of data lost.



If a collector (including the McAfee ePO device) is associated with a Receiver-HA and the Receiver-HA fails over, the collector can't communicate with the Receiver-HA until the switches between the two associate the new MAC address of the failed-over Receiver to the shared IP address. This can take from a few minutes up to a few days, depending on the current network configuration.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the Receiver-HA device, then click the **Properties** icon .
- 2 Select **High Availability | Fail-Over**. The following happens:
 - The ESM instructs the secondary Receiver to start using the shared data source IP and collecting data.
 - The secondary Receiver issues a Cluster Resource Manager (CRM) command to switch the shared IP and MAC, and starts the collectors.
 - The ESM pulls all alert and flow data from the primary Receiver.
 - The ESM marks the secondary Receiver as the primary and marks the primary Receiver as the secondary.

See also

[High Availability Receivers on page 43](#)
[Set up Receiver-HA Devices on page 46](#)
[Reinitialize the secondary device on page 46](#)
[Set up Receiver HA with IPv6 on page 47](#)
[Reset HA devices on page 48](#)
[Replace a failed Receiver on page 49](#)
[Troubleshooting failed Receiver on page 50](#)

Replace a failed Receiver

If a secondary Receiver has a health problem that can't be resolved, it might be necessary to replace the Receiver. When you receive the new Receiver, install it following the procedures in *McAfee ESM Setup and Installation Guide*. When the IP addresses are set and the cables are plugged in, you can proceed to bring the Receiver back into the HA cluster.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **Receiver Properties** for the HA Receiver, then click **Receiver Configuration | Interface**.
- 2 Click the **HA Receiver** tab, then verify that **Setup High Availability** is selected.
- 3 Verify that the IP addresses are correct, then click **Reinitialize Secondary**.

The new Receiver is brought into the cluster and HA mode is enabled.

See also

[High Availability Receivers on page 43](#)
[Set up Receiver-HA Devices on page 46](#)
[Reinitialize the secondary device on page 46](#)
[Set up Receiver HA with IPv6 on page 47](#)
[Reset HA devices on page 48](#)
[Switch Receiver-HA roles on page 49](#)
[Troubleshooting failed Receiver on page 50](#)

Troubleshooting failed Receiver

If a Receiver in an HA setup goes down for any reason, the writing of data sources, global settings, aggregation settings, and others, appears to fail and an SSH error appears.

In fact, the settings roll out to the Receiver that is still functioning, but an error appears because it can't sync with the Receiver that is down. Policy, however, does not roll out. In this situation, you have the following options:

- Wait to roll out policy until a secondary receiver is available and synced.
- Remove the Receiver from HA mode, which causes two to five minutes of down time for the HA cluster during which no events are gathered.

See also

[High Availability Receivers on page 43](#)
[Set up Receiver-HA Devices on page 46](#)
[Reinitialize the secondary device on page 46](#)
[Set up Receiver HA with IPv6 on page 47](#)
[Reset HA devices on page 48](#)
[Switch Receiver-HA roles on page 49](#)
[Replace a failed Receiver on page 49](#)

Archiving Receiver raw data

Configure the Receiver to forward a backup of the raw data to your storage device for long-term storage.

The three types of storage that are supported by the ESM are Server Message Block/Common Internet File System (SMB/CIFS), Network File System (NFS), and Syslog Forwarding. SMB/CIFS and NFS store, in the form of data files, a backup of all raw data sent to the Receiver by data sources that use the email, estream, http, SNMP, SQL, syslog, and remote agent protocols. These data files are sent to the archive every five minutes. Syslog Forwarding sends the raw data for syslog protocols as a continuous stream of combined syslogs to the device configured in the **Syslog Forwarding** section of the **Data Archival Settings** page. The Receiver can forward to only one type of storage at a time; you can configure all three types, but only one type can be enabled to archive data.



This feature doesn't support Netflow, sflow, and IPFIX data source types.

See also

[Event Receiver settings on page 42](#)
[Define archive settings on page 50](#)

Define archive settings

To store the raw data of syslog messages, you must configure the settings used by the Receiver for archiving.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **Receiver Properties**, then click **Receiver Configuration | Data Archival**.
- 2 Select the share type and enter the information requested.



Port 445 must be opened on the system with the CIFS share to enable a CIFS share connection. Likewise, Port 135 must be opened on the system with the SMB share for an SMB connection to be established.

- 3 When you are ready to apply the changes to the Receiver device, click **OK**.

Table 3-22 SMB/CIFS Share Option definitions

Option	Definition
Share Type	Select the SMB or CIFS share type.
IP Address	Type the IP address of the share.
Share Name	Type the name of the share.
Path	Type the subdirectory on the share where the archived data must be stored (for example, TMP/Storage). If storage is in the root directory of the share, no path is required.
Username and Password	Type a valid user name to connect to the share, then the password for the user account being used while connecting to the share. <div> Do not use commas in the password when connecting to an SMB/CIFS share.</div>
Connect	Click to test the connection.

Table 3-23 NFS Share Option definitions

Option	Definition
IP Address	Type the IP Address of the mount point, then the name of the mount point.
Mount Point	Type the name of the mount point.
Path	Type the subdirectory on the share where the archived data should be stored (for example, TMP/Storage). If storage will be in the root directory of the share, no path is required.
Connect	Click to test the connection.

Table 3-24 Syslog Forwarding Share Option definitions

Option	Definition
IPv4 Address or IPv6 Address	Type the IP Address of the syslog server the data stream should be forwarded to.
IPv4 Path or IPv6 Path	Enter the port of the syslog server the data stream should be forwarded to.

See also

[Archiving Receiver raw data on page 50](#)

View source events for correlation event

You can view the source events for a correlation event on the **Event Analysis** view.

Before you begin

A correlation data source must already exist on the ESM (see *Correlation data source* and *Add a data source*).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, expand the Receiver, then click **Correlation Engine**.
- 2 On the view list, click **Event Views**, then select **Event Analysis**.
- 3 On the **Event Analysis** view, click the plus sign (+) in the first column next to the correlation event.



A plus sign appears only if the correlation event has source events.

The source events are listed under the correlation event.

View Receiver throughput statistics


View Receiver usage statistics, which includes the incoming (Collector) and outgoing (parse) data source rates for the last 10 minutes, the last hour, and the last 24 hours.

Before you begin

Verify that you have the Device Management privilege.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select a Receiver, then click the Properties icon .
- 2 Click **Receiver Management | View Statistics | Throughput**.
- 3 View the Receiver statistics.

If incoming rates exceed the output rate by 15 percent, the system flags that row as either critical (in the last 24 hours) or as a warning (in the last hour).
- 4 Filter the data source by selecting the All, Critical, or Warning options.
- 5 Select the unit of measure to display the metrics: by number of kilobytes (KBs) or number of records.
- 6 To refresh the data automatically every 10 seconds, select the **Auto Refresh** checkbox.
- 7 Sort data by clicking the relevant column title.

Receiver data sources

The McAfee Event Receiver enables the collection of security events and network flow data from multi-vendor sources including firewalls, virtual private networks (VPNs), routers, NetFlow, sFlow, and others. Data sources are used to control how log and event data is gathered by the Receiver. You must add data sources and define their settings so they collect the data you need.

The **Data Sources** page is the starting point to manage the data sources for your Receiver device. It provides a way for you add, edit, and delete data sources, as well as import, export, and migrate them. You can also add child and client data sources.

See also

[Add a data source on page 53](#)

[Select Tail File\(s\) data source collection method on page 72](#)

[Set default logging pool on page 34](#)

[Manage data sources on page 55](#)

[Set the date format for data sources on page 66](#)

[Import a list of data sources on page 69](#)


[Move data sources to another system on page 71](#)

Add a data source

Configure the settings for the data sources you need to add to the Receiver to collect data.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the Receiver you want to add the data source to, then click the **Properties** icon .
- 2 On **Receiver Properties**, click **Data Sources | Add**.
- 3 Select the vendor and the model.

The fields you fill out depend on your selections.
- 4 Fill in the information requested, then click **OK**.

The data source is added to the list of data sources on the Receiver, and to the system navigation tree under the Receiver you selected.

Table 3-25 Option definitions




Option	Definition
Data sources table	<p>View the data sources on the system, if they have clients, and what type of data source they are. In addition, it shows whether or not the Receiver processes data for this data source, and the manner it will process the data. The options are:</p> <ul style="list-style-type: none"> • Parsing — Data collected is parsed and inserted into the database. • Logging — The data is sent to the ELM. It is only available if you have an ELM device on your system. • SNMP Trap — The data source accepts standard SNMP traps from any manageable network device that has the capability of sending SNMP traps. These standard traps are: Authentication Failure, Cold Start, EGP Neighbor Loss, Link Down, Link Up and Warm Start. Once these traps are received, an event is generated for that data source. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> If you need to send or receive SNMP traps via IPv6, you have to formulate the IPv6 address as an IPv4 conversion address. For example, converting 10.0.2.84 to IPv6 would look as follows: 2001:470:B:654:0:0:10.0.2.84 or 2001:470:B:654::A000:0254.</p> </div> <p>You can change these settings on the table by selecting and deselecting them. In addition, you can add a storage pool or an SNMP profile by clicking the Logging  or SNMP  icons.</p>
Add	Add a new data source to the Receiver.
Add Child	Add child data sources to an existing data source. This helps to organize your data sources.
Clients	Add client data sources, which extend the number of data sources allowed on a Receiver.
Edit	Make changes to the settings of the selected data source.

Table 3-25 Option definitions *(continued)*

Option	Definition
Remove	Delete the selected data source.
Import	Import a list of data sources saved in .csv format (see <i>Import a list of data sources</i>).
Export	Export a list of the data sources on the system.
Migrate	Reallocate or redistribute data sources between receivers.
Advanced	Upload or view a custom data source definition.
Auto Learn	Set up the Receiver to learn unknown IP addresses automatically.
Rename	Change the names for the user-defined data source entries.
Upload	Upload a file for the selected data source. This is for syslog only.
Write	Write any changes made to the data source settings to the Receiver.

Table 3-26 Option definitions

Option	Definition
Use System Profiles	Select to use a profile to configure this data source. Only SNMP and syslog protocol-based devices can be prepopulated with settings from a profile.
Data Source Vendor, Data Source Model	Select the vendor and model for this data source. When adding an advanced syslog parser (ASP) data source that generates data with encoding other than UTF-8, select Generic as the vendor and Advanced Syslog Parser as the model.
Data Format	Select the parsing method.
Data Retrieval	Select the data collection method. When using SCP, the LANG environment variable must be set to lang=C . If you select SCP File Source , relative paths are not supported. You must define the exact full location. When you select CIFS File Source or NFS File Source , you must select the collection method. See <i>Select Tail File(s) data source collection method</i> for details about this field.
Enabled	Select how the Receiver processes the data. <ul style="list-style-type: none"> If you select Logging, you are asked for details (see <i>Set default logging pool</i>). If you select SNMP Trap (see <i>Processing data source with SNMP Trap</i>), select the profile you want to use on the SNMP Data Source Profile page. If the profile you need is not in the list, click the System Profiles link and add a profile (see <i>Configure profiles</i>).
Name	Type a name for the data source.
IP address, Host Name, Look up	Enter a single IP address or host name. Click Look up to add the host name if you entered an IP address, or to add the IP address if you entered a host name. You can set up a WMI data source with a host name and no IP address.
Remaining fields	Fill in the remaining fields, which vary based on the vendor, device model, data retrieval method, or protocol of the selected device model.
Interface	Configure any of the parent Receiver settings (see <i>Set up interfaces</i>). Make sure that the ports used for data collection are open on the Communication tab. These ports are closed by default, so you must set them up.
Advanced	Add a URL, set up CEF forwarding, or set up this data source for export to another Receiver.

Table 3-27 Option definitions

Option	Definition
Table	Lists the user define rules.
Edit	Click it to rename the selected data source.

See also

Receiver data sources on page 52

Manage data sources on page 55

Set the date format for data sources on page 66

Import a list of data sources on page 69

Move data sources to another system on page 71

Select Tail File(s) data source collection method on page 72

Processing data source with SNMP Trap

The SNMP trap functionality allows a data source to accept standard SNMP traps from any manageable network device that is capable of sending SNMP traps.

These standard traps are:

- Authentication Failure
- Cold Start
- EGP Neighbor Loss
- Link Down
- Link Up and Warm Start



To send SNMP traps through IPv6, you must formulate the IPv6 address as an IPv4 conversion address. For example, converting 10.0.2.84 to IPv6 looks like this:

2001:470:B:654:0:0:10.0.2.84 or 2001:470:B:654::A000:0254.

If you select **SNMP Trap**, there are three options:

- If a profile has not been selected previously, the **SNMP Data Source Profiles** dialog box opens, allowing you to select the profile to be used.
- If a profile has been selected previously, the **SNMP Data Source Profiles** dialog box opens. To change the profile, click the down arrow in the **System Profiles** field and select a new profile.
- If a profile has been selected previously and you want to change it but the drop-down list on the **SNMP Data Source Profiles** dialog box does not include the profile you need, create a data source SNMP profile.

Table 3-28 Option definitions

Option	Definition
System Profiles	Select a profile from the list of existing profiles or click the link and add a new profile that you can then select.
Overwrite existing profile assignment	Select if you want to delete any existing SNMP profile assignment and replace it with this profile.

Manage data sources

You can add, edit, delete, import, export, and migrate data sources, as well as add child and client data sources on the **Data Sources** page.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **Receiver Properties**, then click **Data Sources**.
- 2 View a list of the data sources on the Receiver and perform any of the available options to manage them.
- 3 Click **Apply** or **OK**.

See also

Receiver data sources on page 52

Add a data source on page 53

Set the date format for data sources on page 66

Import a list of data sources on page 69

Move data sources to another system on page 71

Select Tail File(s) data source collection method on page 72

SIEM Collector

The SIEM Collector sends Windows Event Logs to a Receiver, using an encrypted connection.

Without the SIEM Collector, Windows event collection is limited to using the WMI protocol or a third-party agent. In many environments, the security policy locks access to the system so that you can't use WMI.

WMI traffic is clear text and only allows access to logs written to the Windows Event Log. You can't access log files created by other services, such as DNS, DHCP, and IIS, or by using another third-party agent.

Using the SIEM Collector as a standalone or as part of an existing McAfee ePolicy Orchestrator implementation, you can add the WMI functionality to existing McAfee agents.

You can also use the SIEM Collector as a hub to collect logs from other systems, via RPC, without adding the SIEM Collector package to every system.

Other functionality includes:

- Plug-in for user-defined SQL database collection (supports SQL Server and Oracle).
- Plug-in for parsing exported Windows Events in .evt or .evtx formats.
- Plug-in for supporting SQL Server C2 auditing (.trc format).

Integrating vulnerability assessment data

Vulnerability Assessment (VA) on the DEM and Receiver allows you to integrate data that can be retrieved from many VA vendors.

You can use this data in several ways.

- Raise an event's severity based on the endpoint's known vulnerability to that event.
- Set the system to automatically learn assets and their attributes (operating system and services detected).
- Create and manipulate the membership of user-defined asset groups.
- Access summary and drill-down information of the network assets.
- Modify **Policy Editor** configuration such as turn on MySQL signatures if an asset is discovered running MySQL.

You can access VA data generated by the system on predefined views or on custom views that you create. The predefined views are:

- **Dashboard Views | Asset Vulnerability Dashboard**
- **Compliance Views | PCI | Test Security Systems and Processes | 11.2 Network Vulnerability Scans**
- **Executive Views | Critical Vuln on Regulated Assets**

To create a custom view, refer to *Add a custom view*.



If you create a view that includes the **Total Number of Vulnerabilities Count** or **Dial** component, you might see an inflated count of vulnerabilities. This is because the McAfee Threat Intelligence Services (MTIS) feed is adding threats based on the original vulnerability that the VA source reported (see *Asset, threat, and risk assessment*).

The McAfee rules team maintains a rules file that maps a McAfee sigID to a VIN to one or more references to a Common Vulnerabilities and Exposure (CVE) ID, BugTraq ID, Open Source Vulnerability Database (OSVDB) ID, and/or Secunia ID. These vendors report CVE and BugTraq IDs in their vulnerabilities; therefore, CVE and BugTraq IDs are included in this release.

Define a VA system profile

When adding an eEye REM source, the **Add Vulnerability Assessment Source** page gives you the option to use a previously defined system profile. To use this feature, you must first define the profile.

Task

For details about product features, usage, and best practices, click ? or **Help**.



- 1 On the system navigation tree, select a DEM or Receiver device, then click the **Properties** icon .
- 2 Click **Vulnerability Assessment | Add**.
- 3 In the **VA source type** field, select **eEye REM**.
- 4 Click **Use System Profile**.
- 5 Click **Add**, then select **Vulnerability Assessment** in the **Profile Type** field.
- 6 In the **Profile Agent** field, select the SNMP version for this profile.
The fields on the page are activated based on the version selected.
- 7 Fill in the requested information, then click **OK**.

Table 3-29 Option definitions

Option	Definition
Table	View the Receivers and DEMs on the system and their VA sources.
Add	Add a source.
Edit	Change the selected source.
Remove	Delete the selected VA source.
Retrieve	Retrieve the VA data for the selected source.
Write	Write the changes you made to the device.
Upload	(Qualys) If you selected Manual Upload in the Method field when adding a VA source, click this option to upload the file. <div> A Qualys QualysGuard log file upload has a file size limit of 2 GB.</div>

Add a VA source

To communicate with VA sources, add them to the system, add communication parameters for the VA vendor, schedule parameters for how often data is retrieved, and change severity calculations.

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 On the system navigation tree, select a DEM or Receiver device, then click the **Properties** icon .
- 2 Click **Vulnerability Assessment**.
- 3 Add, edit, remove, or retrieve VA sources, and write any changes to the device.
- 4 Click **Apply** or **OK**.

Table 3-30 Option definitions


Option	Definition
Client ID	Type the Frontline client ID number. This field is required for Digital Defense Frontline.
Company Name	On FusionVM, the name of the company that must be scanned. If this field is left blank, all companies that the user belongs to are scanned. If more than 1 company is entered, separate the names with a comma.
Data Retrieval	(Qualys QualysGuard) Select the method to retrieve the VA data. HTTP/HTTPS is the default. The other options are SCP , FTP , NFS , CIFS , and Manual upload . <div>  A Qualys QualysGuard log file manual upload has a file size limit of 2 GB. </div>
Domain	Type the domain of the Windows box (optional, unless your domain controller or server exists within a domain).
Exported scan file directory	The directory where exported scan files reside.
Exported scan file format	The exported scan file format (XML, NBE).
Install directory	The location where Saint was installed on the server. The installation directory for a Saint appliance scanner is <code>/usr/local/sm/</code> .
IP Address	<ul style="list-style-type: none"> For eEye REM: The IP address of the eEye server that are sending trap information. For eEye Retina: The IP address of the client holding exported scan files (.rtd). For McAfee® Vulnerability Manager: The IP address of the server on which it is installed. For Nessus, OpenVAS, LanGuard, and Rapid7 Metasploit Pro: The IP address of the client holding exported scan files. For NGS: The IP address of the system that is storing the Squirrel reports. For Rapid7, Lumension, nCircle, and Saint: The IP address of the respective server.
Mount Directory	If you select nfs in the Method field, the Mount Directory fields are added. Enter the mount directory set when you configured nfs .
Method	The method to use to retrieve the exported scan files (SCP , FTP , NFS , or CIFS mount). LanGuard always uses CIFS .

Table 3-30 Option definitions (continued)


Option	Definition
Password	<ul style="list-style-type: none"> For McAfee Vulnerability Manager: If using Windows authentication mode for SQL Server, the password of the Windows box. If not, the password of the SQL Server. For Nessus, OpenVAS, LanGuard, and Rapid7 Metasploit Pro: The password of SCP or FTP (see <i>Username</i>). For NGS: The password for the SCP and FTP methods. For Qualys and FusionVM: The password for the Qualys Front Office or Fusion VM user name (see <i>Username</i>). For Rapid7 Nexpose, Lumension, nCircle, and Saint: The password to use when connecting to the web server (see <i>Username</i>). For Digital Defense Frontline: The web interface password.
Port	The port Rapid7 Nexpose, Lumension, nCircle, McAfee® Vulnerability Manager, or Saint web server are listening on. The default for Rapid7 Nexpose is 3780, for Lumension is 205, for nCircle is 443, for McAfee Vulnerability Manager is 1433, and for Saint is 22.
Project/Workspace Name	Name of a particular project or workspace, or leave it blank to grab all projects or work spaces.
Proxy IP Address	The IP address of the HTTP proxy
Proxy Password	A password for the proxy user name.
Proxy Port	The port on which the HTTP proxy is listening.
Proxy Username	A user name for the proxy.
Qualys or FusionVM server URL	The URL of the Qualys or FusionVM server to query.
Remote path and share name	For CIFS method Nessus, OpenVAS, eEye Retina, Metasploit Pro, LanGuard, and NGS. You can use back or forward slashes in the path name (for example, Program Files \CIFS\va or /Program Files/CIFS/va).
Schedule Receiver or DEM data retrieval	<p>Indicate the frequency with which you want the VA data to be retrieved from the Receiver or DEM:</p> <ul style="list-style-type: none"> Daily — Select the time you want the data retrieved each day. Weekly — Select the day of the week and the time on that day you want the data retrieved. Monthly — Select the day of the month and the time on that day that you want the data retrieved. <p>If you do not want the data retrieved at a preset time, select Disabled.</p> <div>  eEye REM does not support data retrieval from the source so the data must be retrieved from the Receiver or DEM. </div>
Schedule VA data retrieval	Indicate the frequency with which you want the VA data to be retrieved from the VA source. See <i>Schedule Receiver or DEM data retrieval</i> for details.
Session	Saint: The session data is gathered from. To include all sessions, type All .
SNMP authentication password	If you select authNoPriv or authPriv in the SNMP security level field, this field is active. Enter the password for the authentication protocol selected in the SNMP authentication protocol field.

Table 3-30 Option definitions *(continued)*

Option	Definition
SNMP authentication protocol	If you select authNoPriv or authPriv in the SNMP security level field, this field is active. Select the type of protocol for this source: MD5 or SHA1 (SHA1 and SHA refer to the same protocol type). Make sure that your REM Events Server configuration matches your selection.
SNMP Community	The SNMP community that was set when you configured the REM Events Server.
SNMP privacy password	If you select authPriv in the SNMP security level field, this field is active. Enter the password for the DES or AES privacy protocol. In FIPS mode, AES is the only option available.
SNMP privacy protocol	If you select authPriv in the SNMP security level field, this field is active and you can select either DES or AES. In FIPS mode, AES is the only option available.
SNMP security level	<p>The security level you want to set for this source.</p> <ul style="list-style-type: none"> • noAuthNoPriv — No authentication protocol and no privacy protocol • authNoPriv — Authentication protocol but no privacy protocol • authPriv — Both authentication and privacy protocol. <p>The SNMP authentication and privacy fields become active based on the security level you select. Make sure that your REM Events Server configuration matches your selection.</p>
SNMP user name	The security name in REM Events Server Configuration .
SNMP version	The version of SNMP for the source. The SNMP fields are activated based on the version selected.
SNMPv3 Engine ID	(Optional) The SNMPv3 Engine ID of the trap sender, if an SNMPv3 profile is used.
Sudo password	(Optional) Type the password that is required to access the Saint installation directory (see <i>Use sudo</i>).
Time out	This field allows you to use the default time-out value for a source or provide a specific time-out value. This is useful if you have much VA data from a vendor and the default time-out setting is not allowing you to return all or any of the data. You can increase the time-out value to allow more VA data retrieval time. If you provide a value, it is used for all communications.
Token	(Optional) Authentication token that can be set in the Metasploit Global Settings.
URL	Type the URL to the Digital Defense Frontline server.
Use HTTP Proxy	If you select to use the HTTP proxy, the Proxy IP Address , Proxy Port , Proxy Username , and Proxy Password fields become active.
Use Passive mode	If you select ftp in the Method field, this field becomes active. You must then select when to use passive mode.
Use sudo	Select this option if you have access to the Saint installation directory and want to use this access (see <i>Sudo password</i>).
Use System Profile (eEye REM)	Select whether to use a previously defined profile. If you select this option, all SNMP fields are deactivated. When you select one of the existing system profiles, the fields are populated with the information in the profile selected. To define a profile, see <i>Define a VA system profile</i> .

Table 3-30 Option definitions *(continued)*

Option	Definition
User name	Type the user name for McAfee® Vulnerability Manager. If you are using Windows authentication mode for the SQL Server, enter the user name of the Windows box. If not, it is the user name of the SQL Server. <ul style="list-style-type: none"> • For Nessus, OpenVAS, and Rapid7 Metasploit Pro: The user name of SCP or FTP. • For NGS: The user name for the SCP and FTP methods. • For Qualys or FusionVM: The Front Office or FusionVM user name with which to authenticate. • For Rapid7 Nexpose, Lumension, nCircle, and Saint: The user name to use when connecting to the web server. • For Digital Defense Frontline: The web interface user name.
VA Source Name	Type the name for this source.
Wildcard expression	A wildcard expression used to describe the name of exported scan files. The wildcard expression can use an asterisk (*) or question mark (?) with the standard definition of "wildcard" in a file name. If you have both NBE and XML files, you must specify if you want NBE or XML files in this field (for example, *.NBE or *.XML). If you only use an asterisk (*), you get an error.

Retrieve VA data


Once a source is added, you can retrieve the VA data. There are two ways to retrieve VA data from a source: scheduled or immediate. Either type of retrieval can be performed on all VA sources except eEye REM, which must be scheduled.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **DEM** or **Receiver Properties**, then click **Vulnerability Assessment**.
- 2 Select the VA source, then select one of these options.

To...	Do this...
Retrieve immediately	<ul style="list-style-type: none"> • Click Retrieve. <p>The job runs in the background and you are informed if the retrieval is successful (see <i>Troubleshoot VA retrieval</i> if it is not successful).</p>
Schedule retrieval	<ol style="list-style-type: none"> 1 Click Edit. 2 In the Schedule VA data retrieval field, select the frequency. 3 Click OK. 4 On the Vulnerability Assessment page, click Write to write the changes to the device.

- 3 Click **OK**.
- 4 To view the data, click the **Asset Manager** quick launch icon , then select the **Vulnerability Assessment** tab.



Troubleshooting VA retrieval

When you retrieve VA data, you are informed if it was not successful. Here are some of the reasons the retrieval might be unsuccessful.

This resource...	Causes...
Nessus, OpenVAS, and Rapid7 Metasploit Pro	<ul style="list-style-type: none"> • Empty directory. • Error in the settings. • Data in the directory was already retrieved, so the data isn't current.
Qualys, FusionVM, and Rapid7 Nexpose	Data in the directory was already retrieved, so the data isn't current.
Nessus	If you wrote over an existing Nessus file when you uploaded a new Nessus file to your FTP site, the date of the file remains the same; therefore, when you perform a VA retrieval, no data is returned because it's perceived as old data. To avoid this situation, either delete the old Nessus file off of the FTP site before uploading the new one, or use a different name for the file you upload.

Available VA vendors

The ESM can integrate with these VA vendors.


VA vendor	Version
Digital Defense Frontline	5.1.1.4
eEye REM (REM events server)	3.7.9.1721
eEye Retina	5.13.0, Audits: 2400
 <p>The eEye Retina VA source is like the Nessus data source. You can use scp, ftp, nfs, or cifs to grab the .rtd files. You must manually copy the .rtd files to an scp, ftp, or nfs share to pull them. The .rtd files are normally located in the Retina Scans directory.</p>	
McAfee Vulnerability Manager	6.8, 7.0
Critical Watch FusionVM	4-2011.6.1.48
LanGuard	10.2
Lumension	Support PatchLink Security Management Console 6.4.5 and later
nCircle	6.8.1.6
Nessus	Support Tenable Nessus versions 3.2.1.1 and 4.2 and file formats NBE, .nessus (XMLv2), and .nessus (XMLv1); also, OpenNessus 3.2.1 XML format
NGS	
OpenVAS	3.0, 4.0
Qualys	
Rapid7 Nexpose — Recommended VA partner vendor	
Rapid7 Metasploit Pro — Recommended VA partner vendor	4.1.4-Update 1, file format XML
 <p>You can deduce the severity of a Metasploit exploit that starts with the name Nexpose by adding a Rapid7 VA source to the same Receiver. If it can't be deduced, the default severity is 100.</p>	

VA vendor	Version
Saint	
GFI Languard	
NGS Squirrel	
iScan Online?	
Tripwire/nCircle IPS360?	

Auto create data sources

You can set up the Receiver to create data sources automatically, using the five standard rules that come with the Receiver or rules that you create.

Before you begin

Ensure that auto check is selected on the **Events, Flows & Logs** dialog (**System Properties | Events, Flows & Logs**) or click the **Get Events and Flows** icon  on the actions toolbar to pull events and/or flows.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On **Receiver Properties**, click **Data Sources | Auto Learn**.
- 2 On the **Auto Learn** window, click **Configure**.
- 3 On the **Auto Add Rule Editor** window, ensure that **Enable auto creation** is selected, then select the auto add rules you want the Receiver to use to auto create data sources.
- 4 Click **Run** if you want to apply the selected rules to the existing auto learned data, then click **Close**.

See also

[Set up data source auto-learning on page 64](#)

[Add new auto create rules on page 63](#)

Add new auto create rules

You can add custom rules to be used by the Receiver to auto create data sources.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On **Receiver Properties**, click **Data Sources | Auto Learn | Configure | Add**.
- 2 On the **Configure auto add rule** dialog box, add the data needed to define the rule, then click **OK**.

The new rule is added to the list of auto add rules on the **Auto Add Rule Editor** dialog box. You can then select it so data sources are created when auto learned data meets the criteria defined in the rule.

Table 3-31 Option definitions

Option	Definition
Enable auto creation	Select if you want to automatically create data sources from auto learned data. Auto creation happens whenever alerts are pulled from the Receiver, either manually or automatically by the ESM.
Table	View the auto add rules currently on the Receiver and whether they are enabled. You can enable or disable the rules on this list.

Table 3-31 Option definitions *(continued)*

Option	Definition
Add	Add a new auto add rule.
Edit	Make changes to the selected auto add rule.
Remove	Delete the selected auto add rule.
Run Now	Apply the rules that are enabled to the current list of auto learned data.
Arrow buttons	Move the selected auto add rule up or down on the list to change their order. This is important because auto learned data is matched to the rules in the order they are listed and a data source is created based on the first rule it matches.

Table 3-32 Option definitions

Option	Definition
Description	Type a name that describes this rule.
Type	Select the type of rule from the drop-down list.
Enable	Select if you want to enable this rule.
Auto Learn Matching Criteria column	Define the criteria that the data received must match be added as a data source or client.
Data Source/Client Creation Parameters column	<p>Define the settings for the data source that you want to create if the data matches the criteria.</p> <ul style="list-style-type: none"> Type the name for the data source. This field supports variables to represent IP address, model, and host name. For example, you can type <code>Data source - {MODEL}_{HOST}_{IP}</code>. Select data source or client. If it's a client, select the parent that contains it, then select the client type. Select the vendor, model, time zone, and zone. If you want the data generated by the data source (not clients) to be stored on the ELM, click Storage Pool and select the storage pool.

See also[Auto create data sources on page 63](#)[Set up data source auto-learning on page 64](#)**Set up data source auto-learning**

Set up the ESM to learn IP addresses automatically.

Before you begin

Make sure that ports are defined for Syslog, MEF, and flows (see *Set up the interfaces*).

The firewall on the Receiver opens for the time you designate, so the system can learn a set of unknown IP addresses. You can then add to the system as data sources.



When you upgrade, auto-learning results are deleted from the **Auto Learn** page. If there are auto-learn results you haven't taken action on before upgrading, you must run auto-learning after performing the upgrade to collect those results again.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **Receiver Properties**, then click **Data Sources** | **Auto Learn**.
- 2 Define the settings as needed, then click **Close**.

Table 3-33 Option definitions



Option	Definition
Enable or Disable	<p>Enable or disable auto learning.</p> <p> Receiver ports must match the sources that are sending data or auto learning will not happen.</p> <ul style="list-style-type: none"> • Select the length of time you want auto learning to occur in the appropriate hours field (maximum is 24 hours; 0 is continually), then click Enable. Auto learning will begin and the button will change to Disable. When the time expires, the auto-learn feature will be disabled and the table will be populated with the IP addresses that were found. <p> When using auto learning for MEF, you can't add data sources that are auto learned using a host ID.</p> <ul style="list-style-type: none"> • Stop the process before collection is completed — Click Disable. Data collection will stop but the data collected to that point is processed. • Wait until the process is completed — Data is collected for the specified period of time. The data is processed and is added to the table. <p>All information retrieved is stored on the ESM until you enable auto learning again.</p> <p>You can navigate away from the Auto Learn page and auto learning will continue for the period of time you selected. The Current Status fields will display what is occurring in the auto-learning process.</p> <ul style="list-style-type: none"> • Auto learn stopped — It is not occurring at this time. This can mean auto learning has not been requested or learning and processing that was requested has been completed. • Collecting data — Auto learning has been enabled and is currently collecting the data. This will occur for the period of time you specified. • Processing auto-learned data — The system is processing the data that was collected. This occurs after the data has been collected for the time that you specified. • An error has occurred — An error occurred while data was being collected or processed.
Configure	Set up rules so the IP addresses that are collected can be added as data sources automatically if they meet the criteria defined in the rule.
Table	View the IP addresses of the data sources that have been auto learned. Each one is given a name which consists of the IP address and Auto learned, and lists the format of logs. The system also makes an attempt to match the data source type.

Table 3-33 Option definitions *(continued)*

Option	Definition
Add	<p>Add auto learned IP addresses as data sources.</p> <ol style="list-style-type: none"> 1 Select one or more IP addresses of the same type on the table, then click Add. 2 On the Auto Learned Sources page, select one of the options: 3 Click OK. One of the following occurs: <ul style="list-style-type: none"> • If the selected IP addresses do not have a name associated with them, you are asked if you want to add a prefix to the selected addresses. <ul style="list-style-type: none"> – If you click No, the IP addresses are used as the names for these data sources. – If you click Yes, the Name Prefix page opens. Enter a name and click OK. The names of these data sources will consist of the name you added and the IP address. • If the selected IP addresses have names, the data sources are added to the list on the Data Sources page.
Edit Name	Edit the default name of the selected item. The name field has a limit of 50 characters. Each name must be unique.
Remove	Delete the selected IP addresses from the list. The list isn't saved until Auto Learn is closed.
Change Type	Change the type of the selected IP address. You would do this if the type suggested by the system is wrong. Viewing the packet can give you the information you need to determine the correct type
Refresh	Reload the data on the page, changing the auto learned data and the status of syslog, MEF, or Netflow auto learning.
Show Packet	Click to view the packet for the selected data source.

Table 3-34 Option definitions


Option	Definition
Create data sources for the selected auto-learned items	Creates new data sources for each of the selected auto-learned sources. If more information is required for one of the sources, the Add Data Source page opens allowing you to add the information.
Create client for existing data sources or create a new data source with clients	<p>The following options are available:</p> <ul style="list-style-type: none"> • Client match on type: If a data source exists that matches the selected IP, the items are added to it as match-by-type client data sources. If a data source matching the selected IP doesn't exist, one is created. The remaining items are added to it as match-by-type client data sources. • Client match on IP: This option allows you to select the data source to which you want to add this IP as a client. When you select this option, the drop-down list becomes active. If there are one or more data sources that match this IP, they are listed. If there aren't any, the only option available is None - create new data source. Select the data source you want to add this IP to as a client, then click OK.

See also[Auto create data sources on page 63](#)[Add new auto create rules on page 63](#)**Set the date format for data sources**

Select the format for dates included in data sources.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select a Receiver, then click the **Add data source** icon .
- 2 Click **Advanced**, then make a selection in the **Date Order** field:
 - **Default** - Uses the default date order (month before day). When using client data sources, clients using this setting will inherit the date order of the parent data source.
 - **Month before day** - The month goes before the day (04/23/2014).
 - **Day before month** - The day goes before the month (23/04/2014).
- 3 Click **OK**.

See also

[Receiver data sources on page 52](#)

[Add a data source on page 53](#)

[Manage data sources on page 55](#)

[Import a list of data sources on page 69](#)

[Move data sources to another system on page 71](#)

[Select Tail File\(s\) data source collection method on page 72](#)

Add a child data source

You can add child data sources to help you organize your data sources.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **Receiver Properties**, then click **Data Sources**.
- 2 On the data sources table, click the data source you want to add a child to.
- 3 Click **Add Child**, then fill out the fields as you would for a parent data source.
- 4 Click **OK**.

The data source is added as a child below the parent data source on the table and on the system navigation tree.

Table 3-35 Option definitions

Option	Definition
Data Source Vendor	Select the vendor for the auto learned data source or client.
Data Source Model	Select the model for the data source or client.
Time Zone	Select the time zone for the data source or client.

Client data sources

You can extend the number of data sources allowed on a Receiver by adding client data sources. For data sources with a syslog, ASP, CEF, MEF, NPP, and WMI collector, you can add up to 32,766 data source clients.



If the data source is already a parent or child, or if it is a WMI data source and **Use RPC** is selected, this option is not available.

You can add more than one client data source with the same IP address and use the port number to differentiate them. This allows you to segregate your data using a different port for each data type, then forward the data using the same port it came into.

When you add a client data source (see *Client data sources* and *Add a client data source*), you select whether to use the parent data source port or another port.

Client data sources have these characteristics:

- They don't have VIPS, Policy, or Agent rights.
- They aren't displayed on the **Data Sources** table.
- They appear on the system navigation tree.
- They share the same policy and rights as the parent data source.
- They must be in the same time zone because they use the parent's configuration.



Client WMI data sources can have independent time zones because the time zone is determined by the query sent to the WMI server.

See also

[Add a client data source on page 68](#)

Add a client data source

To increase the number of data sources allowed on the ReceiverAdd a client to an existing data source .

Before you begin

Add the data source to the Receiver (see *Add a data source*).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **Receiver Properties**, then click **Data Sources**.
- 2 Select the data source that you want to add the client to, then click **Clients**.

The **Data source clients** page lists the clients that are currently part of the selected data source.

- 3 Click **Add**, fill in the information requested, then click **OK**.

Events go to the data source (parent or client) that is more specific. For example, you have two client data sources, one with an IP address of 1.1.1.1 and the second with an IP address of 1.1.1.0/24, which covers a range. Both are the same type. If an event matches 1.1.1.1, it goes to the first client because it is more specific.

Table 3-36 Option definitions

Option	Definition
Clients table	View the clients that are part of the data source selected on the Data Sources table.
Search	If you are searching for a specific client, type the client name in the field and click Search .
Add	Click to add a client to the data source.
Edit	Click to edit the selected client.
Remove	Click to delete the selected client.

Table 3-37 Option definitions

Option	Definition
Name	Type a name for this client.
Time Zone	Select the time zone this client data source is in.
Date Order	Select the format for the date: month before day or day before month.
IP Address, Host Name	Type the IP address or host name for the client. You can have more than one client data source with the same IP address. The port is used to differentiate them.
Require syslog TLS	Select to use Transport Layer Security (TLS) encryption protocol for syslog.
Port	Select whether you want the client to use the same port as its parent or another listed port.
Match by type	Select to match clients by type, then select the vendor and model of this client.

See also

[Client data sources on page 68](#)

Locate a client

The **Data source clients** page lists all the clients on the system. Because you can have more than 65,000 clients, a search feature is provided so that you can locate a specific one, if needed.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **Receiver Properties**, then click **Data Sources | Clients**.
- 2 Enter the information you want to search for, then click **Search**.

Import a list of data sources

The **Import** option on the **Data Sources** page allows you to import a list of data sources saved in .csv format. This eliminates the need to add, edit, or remove each data source individually.

You use this option in two situations:

- To import raw data source data copied from a Receiver in a secured location to a Receiver in an unsecured location. If this is what you are doing, see *Move data sources*.
- To edit the data sources on a Receiver by adding data sources to the existing list, editing existing data sources, or removing existing data sources. If this is what you need to do, follow these steps.

Task

For details about product features, usage, and best practices, click ? or **Help**.

1 Export a list of the data sources currently on the Receiver.

- a On the system navigation tree, select **Receiver Properties**, then click **Data Sources**.
- b Click **Export**, then click **Yes** to confirm the download.
- c Select the location for the download, change the file name if needed, then click **Save**.

The list of existing data sources is saved.

- d Access and open this file.

A spreadsheet opens listing the data for the data sources currently on the Receiver (see *Spreadsheet fields when importing data sources*).

2 Add, edit, or remove data sources on the list.

- a In column A, specify the action to be taken with that data source: add, edit, or remove.
- b If you are adding or editing data sources, enter the information in the spreadsheet columns.



You can't edit the policy or the name of the data source.

- c Save the changes made to the spreadsheet.



You can't edit a data source to make it a data source from a client data source or the other way around.

3 Import the list to the Receiver.

- a On the system navigation tree, select **Receiver Properties**, then click **Data Sources**.
- b Click **Import**, then select the file and click **Upload**.



You can't change the policy or the name of the data source

The **Import Data Sources** page opens, listing the changes that have been made to the spreadsheet.

- c To import the changes, click **OK**.
The changes that are formatted correctly are added.
- d If there are errors in the formatting of the changes, a **Message Log** describes the errors.
- e Click **Download Entire File**, then click **Yes**.
- f Select the location for the download to be saved, change the name of the file if needed, then click **Save**.
- g Open the file that downloaded.
It lists the data sources that have errors.
- h Correct the errors, then save and close the file.

- i Close **Message Log** and **Import Data Sources**, then click **Import** and select the file that you saved.

Import Data Sources lists the data sources that you corrected.

- j Click **OK**.

Table 3-38 Option definitions

Option	Definition
Upload	Click and browse to the .nps file of custom data source definitions that you want to add to your ESM. This file is generated by McAfee.
View	Click to view the data source definitions that have been installed.

See also

[Receiver data sources on page 52](#)

[Add a data source on page 53](#)

[Manage data sources on page 55](#)

[Set the date format for data sources on page 66](#)

[Move data sources to another system on page 71](#)

[Select Tail File\(s\) data source collection method on page 72](#)

Migrate data sources to another Receiver

You can reallocate or redistribute data sources between Receivers on the same system.

This can be useful if you purchase a new Receiver and want to balance the data sources and associated data between the two Receivers, or if you purchase a larger replacement Receiver and need to transfer the data sources from the current Receiver to the new one.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **Receiver Properties** for the Receiver with the data sources, then click **Data Sources**.
- 2 Select the data sources to be migrated, then click **Migrate**.
- 3 Select the new Receiver in the **Destination Receiver** field, then click **OK**.

Table 3-39 Option definitions

Option	Definition
Destination Receiver	Lists all the Receivers on the ESM. Select the Receiver that you want to move the selected data sources to.

Move data sources to another system

To move data sources from one Receiver to another on a different system, you must select the data sources to be moved, save them and their raw data to a remote location, then import them to the other Receiver.

Before you begin

To perform this function, you must have device management rights on both Receivers.

Use this process to move data sources from a Receiver located in a secured location to a Receiver in an unsecured location.

There are limitations when exporting data source information:

- You can't transport flow data sources (for example, IPFIX, NetFlow, or sFlow).
- The source events of correlated events do not display.
- If you make a change to the correlation rules on the second Receiver, the correlation engine doesn't process those rules. When the correlation data is transported, it inserts those events from the file.

To...	Do this...
Select the data sources and remote location	<ol style="list-style-type: none"> 1 On the system navigation tree, select Receiver Properties, then click Data Source. 2 Select the data source, then click Edit. 3 Click Advanced, then select Export in NitroFile. <div data-bbox="521 573 565 617" data-label="Image"></div> <div data-bbox="586 579 1315 611" data-label="Text">The data is exported to a remote location and is configured using profile.</div> 4 Click OK. <p>From now on, the raw data generated by this data source is copied to the remote share location.</p>
Create raw data file	<ol style="list-style-type: none"> 1 Access the remote share location where the raw data is saved. 2 Save the raw data that has been generated in a location that allows you to move the file to the second Receiver (such as a jump drive that you can carry to the unsecured location).
Create a file that describes the data sources	<ol style="list-style-type: none"> 1 On the system navigation tree, select Receiver Properties, then click Data Source Import. 2 Locate the file of data sources you moved and click Upload. 3 On the Remote share profile list, select the location where you saved the raw data files. If the profile isn't listed, click Remote share profile and add the profile. 4 Click OK. <p>The data sources are added to the second Receiver and will access the raw data through the remote share profile.</p>
Import raw data and data source files	<ol style="list-style-type: none"> 1 On the system navigation tree, access Data Sources on the second Receiver, then click Import. 2 Locate the file of data sources you moved and click Upload. The Import Data Sources page lists the data sources to be imported. 3 On the Remote share profile list, select the location where you saved the raw data files. If the profile is not listed, click Remote share profile and add the profile (see <i>Configure profiles</i>). 4 Click OK.

See also

[Receiver data sources on page 52](#)

[Add a data source on page 53](#)

[Manage data sources on page 55](#)

[Set the date format for data sources on page 66](#)

[Import a list of data sources on page 69](#)

[Select Tail File\(s\) data source collection method on page 72](#)

Select Tail File(s) data source collection method


If you select **NFS File Source** or **CIFS File Source** in the **Data Retrieval** field when adding a data source, you must choose a collection method.

The options are:

- **Copy File(s)** — Whole logs are copied from the remote share to the Receiver to be processed. If the log files are large and are updated with new information infrequently, copying the whole log file can be inefficient and time consuming.
- **Tail File(s)** — Logs are read remotely and only new events are read. Each time the log is read, it reads from the position where it stopped previously. If the file changes significantly, this is detected and the whole file is reread from the beginning.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click the Receiver, then click the **Add data source** icon  on the actions toolbar.
- 2 Provide the information requested, selecting **CIFS File Source** or **NFS File Source** in the **Data Retrieval** field.
- 3 In the **Collection Method** field, select **Tail File(s)**, then fill in the these fields:
 - **Multiline Delimited Logs** — Select to specify if the events have dynamic length.
 - **Event Delimiter** — Enter a string of characters that signal the end of an event and the beginning of another. These delimiters vary greatly and depend on the type of log file.
 - **Delimiter is regex** — Select if the value in the **Event Delimiter** field is to be parsed as a regular expression rather than a static value.
 - **Tail Mode** — Select **Beginning** to parse files completely that are encountered on the first run, or **End** to note the file size and collect only new events.
 - **Recurse subdirectories** — Select to read collection from child directories (subdirectories), looking for matches with the wildcard expression field. If not selected, it searches only the parent directory files.
- 4 Fill in remaining fields, then click **OK**.

See also

[Receiver data sources on page 52](#)

[Add a data source on page 53](#)

[Manage data sources on page 55](#)

[Set the date format for data sources on page 66](#)

[Import a list of data sources on page 69](#)

[Move data sources to another system on page 71](#)

Configuration for specific data sources

Some data sources require more information and special configuration settings.

See these sections for details.

- | | |
|---|----------------------------------|
| • Check Point | • Big Fix |
| • IBM Internet Security Systems SiteProtector | • Common Event Format |
| • McAfee ePolicy Orchestrator | • ArcSight |
| • ePolicy Orchestrator 4.0 | • Security Device Event Exchange |
| • NSM-SEIM | • Advanced syslog parser |
| • Syslog Relay Support | • WMI event log |
| • Adiscon | |

You can also refer to the current configuration guides for these data sources in the [Knowledge Center](#).

WMI event log

WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM) as defined by the Distributed Management Task Force (DMTF).

It is the primary management technology for Windows operating systems, permitting management information to be shared between management applications. The ability to obtain management data from remote computers is what makes WMI useful.



WMI is not FIPS-compliant. If you are required to comply with FIPS regulations, do not use this feature.

WMI event logs are set up as a data source and sent through the Receiver. The Receiver polls the Windows server on a set interval and collects the events. The WMI collector can collect events from any event log on the Windows box. By default, the Receiver collects security, administration, and event logs. You have the ability to enter other log files, such as Directory Service or Exchange. The event log data gets collected in the packet data and can be viewed through the event table details.



Administrative or backup operator privileges are required for WMI event logs, except when using Windows 2008 or 2008 R2 if the data source and user are set up correctly (see *Pull Windows security logs*).

These additional devices are supported from the WMI data source:

- McAfee Antivirus
- Windows
- Microsoft ISA Server
- Microsoft Active Directory
- Microsoft SQL Server
- RSA Authentication Manager
- Symantec Antivirus
- Microsoft Exchange



For instructions on setting up syslog WMI through Adiscon, see *Adiscon Set up*.

When you are setting up a WMI data source, the vendor is **Microsoft** and the model is **WMI Event Log**.

Set up to pull Windows security logs

When using Windows 2008 or 2008 R2, Windows security logs can be pulled by users who do not have administrator privileges if the WMI Event Log data source and the user are set up correctly.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Create a new user on the Windows 2008 or 2008 R2 system where you want to read event logs.
- 2 Assign the user to the Event Log Readers group on the Windows system.
- 3 Create a new Microsoft WMI Event Log data source on the McAfee Event Receiver, entering the credentials for the user created in Step 1 (see *Add a data source*).
- 4 Select **Use RPC** box, then click **OK**.

Correlation data source

A correlation data source analyzes data flowing from an ESM and detects suspicious patterns in the data flow. It generates correlation alerts that represent these patterns and inserts these alerts into the Receiver's alert database.

Data interpreted by correlation policy rules, which you can create and modify, represents a suspicious pattern.

Only one correlation data source can be configured on a Receiver, in a similar fashion to configuring syslog or OPSEC. Once you have configured a Receiver's correlation data source, you can roll out the correlation's default policy. You can then edit the base rules in this correlation's default policy, or add custom rules and components and then roll out the policy. You can enable or disable each rule and set the value of each rule's user-definable parameters. For details regarding the Correlation Policy, see *Correlation rules*.

When you are adding a correlation data source, the vendor is **McAfee** and the model is **Correlation Engine**.

When the correlation data source is enabled, the ESM sends alerts to the correlation engine on the Receiver.

Severity and action maps

The severity and action parameters have slightly different usages. The goal with these is to map a value from the syslog message to a value that fits into the system's schema.

- **severity_map** — Severity is shown as a value between 1 (least severe) and 100 (most severe) assigned to events matching the rule. In some cases, the device sending the message may show severity as a number 1–10, or as text (high, medium, low). When this happens, it can't be captured as the severity so a mapping must be created. For example, here is a message coming from McAfee IntruShield that shows severity in text form.

```
<113>Apr 21 07:16:11 SyslogAlertForwarder: Attack NMAP: XMAS Probe (Medium)\000
```

The syntax for a rule using severity mapping would look like this (severity mapping is in bold for emphasis only):

```
alert any any any -> any any (msg:"McAfee Traffic"; content:"syslogalertforwarder";
severity_map:High=99,Medium=55,Low=10; pcre:"(SyslogAlertForwarder)\x3a\s+Attack\s+
([\x27]+\x27([\x28]+\x28"; raw; setparm:application=1; setparm:msg=2;
setparm:severity=3; adsid:190; rev:1;)
```

severity_map: High=99,Medium=55,Low=10. This maps the text to a number in the format we can use.

setparm: severity=3. This says to take the third capture and set it equal to the severity. All setparm modifiers work this way.

- **action_map** — Used just like severity. Action represents the action the third-party device took. The goal with action is to create a mapping that is useful to the end user. For example, here is a failed logon message from OpenSSH.

```
Dec 6 10:27:03 nina sshd[24259]: Failed password for root from 10.0.12.20 port
49547 ssh2
```

```
alert any any any -> any any (msg:"SSH Login Attempt"; content:"sshd";
action_map:Failed=9,Accepted=8;
```

```
pcre:"sshd\x5b\d+\x5d\x3a\s+((Failed|Accepted)\s+password)\s+for\s+((invalid|
illegal)\s+user\s+)?(\S+)\s+from\s+(\S+)\s+(\S+)\s+port\s+(\d+))?"; raw;
setparm:msg=1; setparm:action=2; setparm:username=5; setparm:src_ip=6; adsid:190;
rev:1;)
```

The action (Failed) is mapped to a number. This number represents the different actions we can use in our system. Below is the full list of usable action types.

- | | |
|--------------|------------------|
| • 0 = null | • 20 = stop |
| • 1 = pass | • 21 = noticed |
| • 2 = reject | • 22 = trusted |
| • 3 = drop | • 23 = untrusted |

- 4 = sdrop
- 5 = alert
- 6 = default
- 7 = error
- 8 = success
- 9 = failure
- 10 = emergency
- 11 = critical
- 12 = warning
- 13 = informational
- 14 = debug
- 15 = health
- 16 = add
- 17 = modify
- 18 = remove
- 19 = start
- 24 = false positive
- 25 = alert-reject
- 26 = alert-drop
- 27 = alert-sdrop
- 28 = restart
- 29 = block
- 30 = clean
- 31 = clean-fail
- 32 = continue
- 33 = infected
- 34 = move
- 35 = move-fail
- 36 = quarantine
- 37 = quarantine-fail
- 38 = remove-fail
- 39 = denied

In this example, `Failed` is mapped from the syslog message to 9, which the system reports as `Failure`.

Here is a breakdown of the structure for a rule.

```
Alert any any any -> any any (msg:"Login Attempt"; content:"sshd"; action_map or
severity_map (if you need it); pcre:"your regular expression goes here"; raw;
setparm:data_tag_goes_here; adsid:190; rev:1;)
```

Advanced syslog parser

The Advanced Syslog Parser (ASP) provides a mechanism for parsing data out of syslog messages based on user-defined rules. The rules instruct the ASP how to recognize a given message and where in that message-specific event data resides such as Signature IDs, IP addresses, ports, user names, and actions.

The ASP can be utilized for syslog devices that are not specifically identified in the **Add Data Source** page or when the Source Specific Parser doesn't correctly interpret messages or fully interpret data points related to received events. It is also ideal for sorting through complex log sources such as Linux and UNIX servers. This functionality requires you to write rules (see *Add Rules to the Advanced Syslog Parser*) tailored to your Linux or UNIX environment.

You can add an ASP data source to the Receiver by selecting Syslog as the vendor (see *Add a Data Source*). Once you have done this, follow the device manufacturer's directions to configure your syslog device to send syslog data to the Receiver's IP address.

When you add an ASP source, you must apply a policy before collects event data. If you enable **Generic Syslog Support**, you can apply a policy with no rules and begin generically collecting event data.



Some data sources including Linux and UNIX servers can produce large amounts of non-uniform data that results in the Receiver not properly grouping the similar event occurrence together. This results in an appearance of a large range of different events when in actuality the same event is simply repeating, but with varying syslog data sent to the Receiver.

Adding rules to your ASP allows you to get the most from your event data. The ASP uses a format very similar to Snort.

```
ACTION Protocol Src_ip Src_port -> Dst_ip Dst_port (keyword: option; keyword:
option;...;)
```



When concatenating a literal value with a PCRE subcapture in versions 9.0.0 and later, put the literals in quotes individually if they contain spaces or other characters and leave the PCRE subcapture references unquoted.

Rules are defined as follows.

Section	Field	Description
Rule Header		The rule header contains the Alert action and the any any any format. The rule is: ALERT any any any -> any any
	Action	What to do with the event when a match occurs. Options are: <ul style="list-style-type: none"> • ALERT — Log the event • DROP — Log the event but don't forward • SDROP — Don't log the event or forward • PASS — Forward if defined, but don't log
	Protocol	If the event defines a protocol, then filter the effective match based on the protocol.
	Src/Dst IP	If the event defines a source or destination IP address, then filter the effective match based on that address.
	Src/Dst Port	If the event defines a source or destination port, then filter the effective match based on that port.
Rule Body		The rule body contains the majority of the match criteria and defines how the data must be parsed and logged into the ESM database. Elements of the Rule Body are defined in keyword-option pairs. Some keywords have no following option.
	msg	(Required) The message to associate with this rule. This is the string displayed in the ESM Thin Client for reporting purposes unless overridden with a pcre/setparm detected message (see below). The first work of the msg is the category name followed by actual message (msg: "category rule message").
	content	(Optional — one or more) The content keyword is a non-wildcard text qualifier to pre-filter Events as they pass through the rule set, which can also contain spaces (for example, content: "search 1"; content "something else")
	procname	On many UNIX and Linux systems, the process name (and process ID) is part of a standardized syslog message header. The procname keyword can be used to filter Event matches for the Rule. Used to exclude or filter Event matches where two processes on a Linux or UNIX server may have similar or the same message text.
	adsid	The data source ID to use. This value overrides the Default Rule Assignment in the data source editor.
	sid	Signature ID of the Rule. This is the match ID used in the ESM Thin Client unless overridden with a pcre/setparm detected sid.
	rev	Rule revision. Used to track changes.
	severity	Value between 1 (least severe) and 100 (most severe) assigned to events matching the rule.
	pcre	The PCRE keyword is a Perl Compatible Regular Expression match against incoming events. The PCRE is quote delimited and all occurrences of "/" is treated as a normal character. Content in parentheses is held for the use of the setparm keyword. The PCRE keyword can be modified by nocase, nomatch, raw and setparm keywords.
	nocase	Causes the PCRE content to be matched whether the case matches or not.

Section	Field	Description
	nomatch	Inverts the PCRE match (equivalent to !~ in Perl).
	raw	Compare the PCRE to the entire syslog message including header data (Facility, daemon, date, host/IP, process name and process ID). Normally the header is not used in the PCRE match.
	setparm	Can occur more than once. Each set of parentheses in the PCRE is assigned a number in order of occurrence. Those numbers can be assigned to data tags (for example: setparm:username=1). This takes the captured text in the first set of parentheses and assigns it to the user name data tag. Recognized tags are listed in the table below.

Tag	Description
* sid	This captured parameter overrides the matched rule's sid.
* msg	This captured parameter overrides the matched rule's message or name.
* action	This captured parameter indicates what action the third-party device took.
* protocol	
* src_ip	This replaces the syslog source's IP which is the default source IP of an event.
* src_port	
* dst_ip	
* dst_port	
* src_mac	
* dst_mac	
* dst_mac	
* genid	This is used to modify the sid as stored in the database, used for non-McAfee snort matches in snort preprocessors.
* url	Reserved, but not used yet.
* src_username	First/source user name.
* username	Alternate name for src_username.
* dst_username	Second/destination user name.
* domain	
* hostname	
* application	
* severity	Must be an integer.
* action map	Allows you to map specific actions of your product to the McAfee actions. The action map is case sensitive. Example: alert any any any -> any any (msg:"OpenSSH Accepted Password"; content:"Accepted password for "; action_map:Accepted=8, Blocked=3; pcre:"(Accepted)\s+password\s+for\s+(\S+)\s+from\s+(\d+\.\d+\.\d+\.\d+)\s+port\s+(\d+)"; setparm:action=1; sid:31; rev:1;)). See <i>Severity and Action Map</i> for details.
* severity map	Allows you to map specific severities of your product to the McAfee severity. Like the action map, the severity map is case sensitive. Example: alert any any any -> any any (msg:"OpenSSH Accepted Password"; content:"Accepted password for "; severity_map:High=99, Low=25, 10=99, 1=25; pcre:"(Accepted)\s+password\s+for\s+(\S+)\s+from\s+(\d+\.\d+\.\d+\.\d+)\s+port\s+(\d+)"; setparm:action=1; sid:31; rev:1;))pri(?:\x3d \x3a)\s*(?:p\x5f)?(?:^\x2c)+). See <i>Severity and Action Map</i> for details.

Tag	Description
* var	<p>This is another way to use setparms. The beneficial use, however, is the use of creating one value from multiple captures of multiple PCREs. You can create more than one PCRE that captures only a small portion of your string rather than one large PCRE with multiple captures. Here's an example of capturing a user name, domain, and creating an email address to store in the objectname field.</p> <ul style="list-style-type: none"> • Syntax = var:field=\${PCRE:Capture} • PCRE = not the actual PCRE but the number of the pcre. If your rule has two PCRE's you would have a PCRE of 1 or 2. • Capture = not the actual capture but the number (first, second or third capture [1,2,3]) • Sample Message: A man named Jim works for McAfee. • PCRE: (Jim).*(McAfee) • Rule: alert any any any -> any any (msg:"Var User Jim"; content:"Jim"; pcre:"(Jim)"; pcre:"(McAfee)"; var:src_username=\${1:1}; var:domain=\${2:1}; var:objectname=\${1:1}@\${2:1}.com raw; classtype:unknown; adsid:190; sev:25; sid:610061000; rev:1; normID:1209008128; gensys:T;) • Mapped Source User: Jim • Mapped Domain: McAfee • Mapped objectname: Jim@McAfee.com
* sessionid	This is an integer.
* commandname	This is a string value.
* objectname	This is a string value.
* event_action	This tag is used to set a default action. You can't use event_action and action_map in the same rule. For example, if you had an event for a Successful Login you could use the event_action tag and default the action to success (for example, event_action:8;).

Tag	Description
* firsttime_fmt	Used to set the first time of the event. See list of formats.
* lasttime_fmt	<p>Used to set the last time of the event. See list of formats. You can use this with a setparm or a var (var:firsttime="{1:1}" or setparm:lasttime="1"). For example:</p> <pre> alert any any any -> any any (msg:"SSH Login Attempt"; content:"content"; firsttime_fmt:"%Y-%m-%dT%H:%M:%S.%f"; lasttime_fmt:"%Y-%m-%dT%H:%M:%S.%f" pcrc:"PCRE goes here; raw; setparm:firsttime=1; setparm:lasttime=1; adsid:190; rev:1;) </pre> <p>For current formats supported, see http://pubs.opengroup.org/onlinepubs/009695399/functions/strptime.html for more detail.</p> <p>%Y - %d - %m %H : %M : %S %m - %d - %Y %H : %M : %S %b %d %Y %H : %M : %S %b %d %Y %H - %M - %S %b %d %H : %M : %S %Y %b %d %H - %M - %S %Y %b %d %H : %M : %S %b %d %H - %M - %S %Y %H : %M : %S %Y %H - %M - %S %m - %d - %Y %H : %M : %S %H - %M - %S</p> <p>%Y is 4-digit year %m is month number (1-12) %d is date (1-31) %H is hours (1-24) %M is minutes (0-60) %S is seconds (0-60) %b is month abbreviation (jan, feb)</p>

This is an example of a rule that identifies a password based on OpenSSH login and pulls from the event's source IP address, source port, and user name:

```

alert any any any -> any any (msg:"OpenSSH Accepted Password";content:"Accepted
password for ";pcrc:"Accepted\s+password\s+for\s+(\S+)\s+from\s+(\d+\.\d+\.\d+\.\d+)\s
+port\s+(\d+) ";setparm:username=1;setparm:src_ip=2;setparm:src_port=3;sid:31;rev:1;)

```


For PCRE Resources Online, visit <http://perldoc.perl.org/perlre.html>.

Add an ASP data source with different encoding

The ESM reads UTF-8 encoded data. If you have an ASP data source that generates data with different encoding, you must indicate that when adding the data source.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, click a Receiver, then click the **Add Data Source** icon .
- 2 Select **Generic** in the **Data Source Vendor** field, then **Advanced Syslog Parser** in the **Data Source Model** field.
- 3 Enter the information requested, and select the correct encoding in the **Encoding** field.

The data from this data source is formatted so that it can be read by the Receiver when it is received.

Security Device Event Exchange (SDEE)

The SDEE format describes a standard way of representing events generated by various types of security devices. The SDEE specification indicates that SDEE events are transported using the HTTP or HTTPS protocols. HTTP servers using SDEE to provide event information to clients are called SDEE providers, while the initiators of the HTTP requests are called SDEE clients.

Cisco has defined some extensions to the SDEE standard, calling it the CIDEE standard. The Receiver can act as an SDEE client requesting CIDEE data generated by Cisco intrusion prevention systems.

Unlike some of the other types of data sources supported by the Receiver, SDEE uses a "pull" model instead of a "push" model. This means that periodically the Receiver contacts the SDEE provider and requests any events generated since the time of the last event was requested. Each time events are requested from the SDEE provider, they are processed and stored into the Receiver's event database, ready to be retrieved by the ESM.

You can add a SDEE provider to a Receiver as a data source by selecting Cisco as the vendor and IOS IPS (SDEE) as the data source model (see *Add a data source*).

The Receiver is able to extract this information from an SDEE/CIDEE event:

- Source and destination IP addresses
- Source and destination ports
- Protocol
- Event time
- Event count (CIDEE provides a form of event aggregation, which the Receiver honors)
- Signature ID and sub-ID
- The ESM event ID is calculated from the SDEE signature ID and the CIDEE sub-signature ID using the following formula:

$$\text{ESMI ID} = (\text{SDEE ID} * 1000) + \text{CIDEE sub-ID}$$

So, if the SDEE signature ID is 2000 and the CIDEE sub-signature ID is 123, the ESMI event ID would be 2000123.

- Vlan
- Severity
- Event description
- Packet contents (if available).


If the Receiver is connecting to the SDEE provider for the first time, the current date and time is used as a starting point for requesting events. Future connections request all events since the last successful pull.

Add an ArcSight data source

Add data sources for an ArcSight device.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the Receiver node .
- 2 Click the **Add Data Source** icon  on the actions toolbar.
- 3 Select **ArcSight** in the **Data Source Vendor** field, then select **Common Event Format** in the **Data Source Model** field.
- 4 Type a name for the data source, then type the ArcSight IP address.
- 5 Complete the remaining fields (see *Add a Data Source*).
- 6 Click **OK**.
- 7 Set up a data source for each source that forwards data to the ArcSight device.

The data received from ArcSight is parsed so it can be viewed on the ESM console.

Common Event Format (CEF)

ArcSight currently converts events from 270 data sources to Common Event Format (CEF) using smart connectors. CEF is an interoperability standard for event- or log-generating devices. It contains the most relevant device information and makes it easy to parse and use events.

The event message doesn't need to be explicitly generated by the event producer. The message is formatted using a common prefix composed of fields delimited by a bar (|) character. The prefix is mandatory and all specified fields must be present. Additional fields are specified in the extension. The format is:

```
CEF:Version|Device Vendor|Device Product|Device Version|deviceEventClassId|Name|Severity|Extension
```

The extension part of the message is a placeholder for additional fields. Following are definitions for the prefix fields:

- **Version** is an integer and identifies the version of the CEF format. Event consumers use this information to determine what the fields represent. Currently only version 0 (zero) is established in the above format. Experience might show that other fields must be added to the "prefix" and therefore require a version number change. Adding new formats is handled through the standards body.
- **Device Vendor**, **Device Product**, and **Device Version** are strings that uniquely identify the type of sending device. No two products may use the same device-vendor and device-product pair. There is no central authority managing these pairs. Event producers have to ensure that they assign unique name pairs.
- **DeviceEventClassId** is a unique identifier per event-type. This can be a string or an integer. DeviceEventClassId identifies the type of event reported. In the intrusion detection system (IDS) world, each signature or rule that detects certain activity has a unique deviceEventClassId assigned. This is a requirement for other types of devices as well, and helps correlation engines deal with the events.
- **Name** is a string representing a human-readable and understandable description of the event. The event name should not contain information that is specifically mentioned in other fields. For example: "Port scan from 10.0.0.1 targeting 20.1.1.1" is not a good event name. It must be: "Port scan." The other information is redundant and can be picked up from the other fields.

- **Severity** is an integer and reflects the importance of the event. Only numbers from 0 to 10 are allowed, where 10 indicates the most important event.
- **Extension** is a collection of key-value pairs. The keys are part of a predefined set. The standard allows for including additional keys as outlined later. An event can contain any number of key-value pairs in any order, separated by spaces. If a field contains a space, such as a file name, this is okay and can be logged in exactly that manner. For example:

```
fileName=c:\Program Files\ArcSight is a valid token.
```

Here is a sample message to illustrate appearance:

```
Sep 19 08:26:10 zurich CEF:0|security|threatmanager|1.0|100|worm successfully stopped|
10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

If you use NetWitness, your device needs to be configured correctly to send the CEF to the Receiver. By default, the CEF format when using NetWitness will look as follows:

```
CEF:0|Netwitness|Informer|1.6|{name}|{name}|Medium | externalId={#sessionid}
proto={#ip.proto} categorySignificance=/Normal categoryBehavior=/Authentication/Verify
categoryDeviceGroup=/OS categoryOutcome=/Attempt categoryObject=/Host/Application/
Service act={#action} deviceDirection=0 shost={#ip.host} src={#ip.src}
spt={#tcp.srcport} dhost={#ip.host} dst={#ip.dst} dport={#tcp.dstport}
duser={#username} dproc=27444 fileType=security cs1={#did} cs2={#password} cs3=4 cs4=5
cn1={#rid} cn2=0 cn3=0
```

The correct format requires you to change "dport" above to "dpt."

Adiscon setup

Syslog WMI is supported through Adiscon.

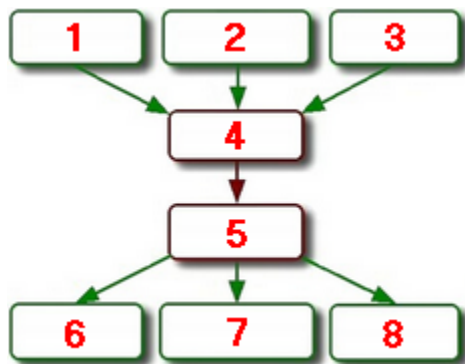
The following format string must be used in Event Reporter for the Microsoft Adiscon Windows Events Data Source to work properly:

```
%sourceproc%,%id%,%timereported:::uxTimeStamp%,%user%,%category%,%Param0%;%Param1%;
%Param2%;%Param3%;%Param4%;%Param5%;%Param6%;%Param7%;%Param8%;%Param9%;%Param10%;
%Param11%;%Param12%;%Param13%;%Param14%;%Param15%
```

Syslog relay support

Forwarding events from various devices through a syslog relay server to the Receiver requires additional steps.

You must add a single syslog relay data source to accept the stream of data and additional data sources. This allows the Receiver to split up the stream of data into the originating data sources. Syslog-ng and Splunk are supported. This diagram describes this scenario:



- | | |
|---------------------------|------------------------------------|
| 1 Cisco ASA Device | 5 Data Source 1 — Syslog Relay |
| 2 SourceFire Snort Device | 6 Data Source 2 — Cisco ASA |
| 3 TippingPoint Device | 7 Data Source 3 — SourceFire Snort |
| 4 Syslog Relay | 8 Data Source 4 — TippingPoint |

Using this scenario as an example, you must set up the syslog relay data source (5) to receive the stream of data from the syslog relay (4), selecting **syslog** in the **Syslog relay** field. Once the syslog relay data source is set up, add the data sources for the individual devices (6, 7, and 8), selecting **None** in the **Syslog relay** field, because this device is not a syslog relay server.



The **Upload Syslog Messages** feature does not work on a syslog relay setup.

The header on the syslog must be configured to look like the following example: 1 <123> 345 Oct 7 12:12:12 2012 mcafee.com httpd[123]

where

1 =	syslog version (optional)
345 =	syslog length (optional)
<123> =	facility (optional)
Oct 7 12:12:12 2012 =	date; hundreds of formats are supported (required)
mcafee.com	hostname or ip address (ipv4 or ipv6) (required)
httpd =	application name (optional)
[123]	application pid (optional)
:	a colon (optional)



The host name and data fields can appear in either order. An IPv6 address can be enclosed in brackets [].

Run NSM-SIEM configuration tool

Prior to setting up an NSM data source, you must run the NSM-SIEM Configuration Tool.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- Download the configuration tool.
 - Browse to the McAfee Product Download website.
 - Enter the customer grant number that was provided to you, in the **Download My Products** search box.
 - Click **Search**. The product update files are found under the MFE <product name> <version> downloads link.
 - Read the McAfee EULA and click **I Agree**.
 - Download the **NSM-SIEM Configuration Tool** files.
- Run the configuration tool on the NSM server.

The tool must find the default path to the NSM. If it does not locate it, browse to it.
- Enter the NSM SQL user, password, and database name that was entered in the install of NSM.
- Enter the SIEM user name and password on the data source and Receiver IP address where the data source is added.

These are entered on the data source screen.

Setting up ePolicy Orchestrator

You can set up multiple ePolicy Orchestrator data sources all pointing to the same IP address with different names in the database name field.

This allows you to set up as many ePolicy Orchestrator data sources as you choose and have them all point to a different database on your central server. Fill in the **User ID** and **Password** fields with the information that provides access to the ePolicy Orchestrator database, and the **Version** field with the version of the ePolicy Orchestrator device. The default port is 1433.



Database Name is required. If the database name contains a dash, you must enclose the name in brackets (for example, [ePO4_WIN-123456]).

The **ePO Query** option allows you to query the ePolicy Orchestrator device and create client data sources. If the default **Match by type** is selected in the **Use client data sources** field and you click **ePO Query**, the ePolicy Orchestrator device is queried and any supported ePolicy Orchestrator products are added as client data sources.

These products are supported if they are fully integrated into ePolicy Orchestrator:

- ANTISPYWARE
- DLP
- EPOAGENT
- GSD
- GSE
- HOSTIPS
- MNAC
- POLICYAUDITOR
- SITEADVISOR
- VIRUSCAN
- SOLIDCORE

If **Match on IP** is selected, the ePolicy Orchestrator device is queried and creates client data sources for all the endpoints in the ePolicy Orchestrator database. If more than 256 endpoints exist in the ePolicy Orchestrator database, multiple data sources are created with clients.

McAfee risk assessment data is acquired from ePolicy Orchestrator servers. You can specify multiple ePolicy Orchestrator servers from which to acquire McAfee Risk Advisor data. The McAfee Risk Advisor data is acquired via a database query from the ePolicy Orchestrator SQL Server database. The database query results in an IP versus reputation score list, and constant values for the low reputation and high reputation values are provided. All ePolicy Orchestrator and McAfee Risk Advisor lists merge, with any duplicate IPs getting the highest score. This merged list is sent, with low and high values, to any ACE devices for scoring SrcIP and DstIP fields.

When you add an ePolicy Orchestrator data source and click **OK** to save it, you are asked if you want to use this data source to configure McAfee Risk Advisor data. If you click **Yes**, a data enrichment source and two ACE scoring rules (if applicable) are created and rolled out. To view these, go to the **Enable data enrichment** and **Risk correlation scoring** pages. To use the scoring rules, you must create a risk correlation manager (see *Add a risk correlation manager*).

IBM Internet Security System SiteProtector

The Receiver is capable of retrieving events from an Internet Security Systems (ISS) SiteProtector server by querying the Microsoft SQL Server database SiteProtector used to store its events.

Unlike some of the other types of data sources supported by the Receiver, retrieving events from a SiteProtector server is done using a "pull" model instead of a "push" model. This means that periodically, the Receiver contacts the SiteProtector database and requests any new events since the last event pulled. Each time events are retrieved from the SiteProtector server they are processed and stored in the Receiver's event database, ready to be retrieved by the ESM.

There are two device type options available: **Server** and **Managed Device**. Setting up a data source with the Server device type selected is the minimum requirement to gather events from a SiteProtector server.

Once a SiteProtector Server data source is configured, all events gathered from SiteProtector show up as belonging to that data source, without regard to the actual asset that reported the event to the SiteProtector server. To have events further categorized according to the managed asset that reported the event to SiteProtector, you can set up additional SiteProtector data sources with the **Managed Device** device type selected.

The **Advanced** option at the bottom of the page allows you to define a URL that can be used to launch specific URLs when viewing event data. You can also define a vendor, product, and version to be used for Common Event Format (CEF) event forwarding. These settings are optional.

For the Receiver to query the SiteProtector database for events, the Microsoft SQL Server installation hosting the database used by SiteProtector must accept connections from the TCP/IP protocol.



See your Microsoft SQL Server documentation for steps on how to enable this protocol and define the port used for these connections (the default is port 1433).

When the Receiver is connecting to the SiteProtector database for the first time, new events generated after the current time are retrieved. Future connections request all events that occurred after the last event that was successfully retrieved.

The Receiver extracts this information from a SiteProtector event:

- Source and destination IP addresses (IPv4)
- Source and destination ports
- Protocol
- Event time
- Event count
- Vlan
- Severity
- Event description

Set up Check Point

Set up data sources that cover Provider 1, Check Point High Availability, and most standard Check Point environments.

Your first step is to add the parent Check Point data source (see *Add a data source*). You must add a data source for the log server if your parent data source is not acting as a log server and you have a dedicated log server. Also add child data sources as needed. If you are in a high availability environment, you must add a child data source for each secondary SMS/CMA.

Task


For details about product features, usage, and best practices, click **?** or **Help**.

- 1 Add a parent data source for your SMS/CMA where the OPSEC application/certificate is stored or, if on a Receiver-HA, your primary SMS/CMA.



OPSEC is not FIPS-compliant. If you are required to comply with FIPS regulations, do not use this feature (see *Appendix A*).

- 2 Click **Options**.
- 3 On the **Advanced Settings** page, select the communication method, then type the **Server Entity Distinguished Name** of this data source.
- 4 Click **OK** twice.
- 5 Do the following, if needed:

If you receive this error...	Do the following...
SIC Error for lea: Client could not choose an authentication method for service lea	<ol style="list-style-type: none"> 1 Verify that you selected the correct settings for Use Authentication and Use Encryption when you added the Check Point data source. <div>  <p>If you selected Use Authentication only, the OPSEC client attempts to communicate with the log server using "sslca_clear". If you selected Use Authentication and Use Encryption, the OPSEC client attempts to communicate with the log server using "sslca." If you selected neither, the OPSEC client attempts to communicate with the log server using "none."</p> </div> 2 Verify that the OPSEC application you are using to communicate with the Check Point log server has LEA selected in the Client Entities section. 3 If both of these steps verify correctly, locate the sic_policy.conf file on your Check Point Log Server installation. For example, on a Linux-based R65 system, the file is located in /var/opt/CPshrd-R65/conf. 4 When you determine which communication method (authentication method in the file) allows LEA communication method to the Log Server, select that communication method on the Advanced Settings page as Communication Method.
SIC Error for lea: Peer sent wrong DN: <expected dn>	<ul style="list-style-type: none"> • Provide a string for the Server Entity Distinguished Name text box by entering the string that represents "<expected dn>" in the error message. <p>An alternative is to find the distinguished name for the Check Point Log Server by looking at the Check Point Log Server's network object in the Smart Dashboard UI.</p> <p>The DN of the SMS/CMA will be like that of the DN for the OPSEC app, just replace the first entry with CN=cp_mgmt. For instance consider an OPSEC app DN of CN=mcafee_OPSEC,O=r75..n55nc3. The SMS/CMA DN will be CN=cp_mgmt,O=r75..n55nc3. The DN of the log server would be like this, CN=CPlogserver,O=r75..n55nc3.</p>

- 6 Add a child data source for every firewall, log server, or secondary SMS/CMA that is managed by the parent data source that you set up (see *Add a child data source*).

The device type for all firewall/gateway data sources is **Security Device**. The **Parent Report Console** defaults to the parent data source.

McAfee rulesets

This table lists the McAfee rulesets along with the external data source IDs.

Data Source ID	Display Name	Corresponding RSID	Rule Range
50201	Firewall	0	2,000,000–2,099,999
50202	Custom Firewall	0	2,200,000–2,299,999
50203	Custom Signatures	0	5,000,000–5,999,999
50204	Internal	0	3,000,000–3,999,999
50205	Vulnerability and Exploit	2	N/A
50206	Adult Content	5	N/A
50207	Chat	8	N/A
50208	Policy	11	N/A
50209	Peer to Peer	14	N/A
50210	Multimedia	17	N/A
50211	Alpha	25	N/A

Data Source ID	Display Name	Corresponding RSID	Rule Range
50212	Virus	28	N/A
50213	Perimeter Secure Application	31	N/A
50214	Gateway	33	N/A
50215	Malware	35	N/A
50216	SCADA	40	N/A
50217	MCAFEESYSLOG	41	N/A

Receiver asset sources

An asset is any device on the network that has an IP address. The **Asset** tab on the **Asset Manager** allows you to create assets, change their tags, create asset groups, add asset sources, and assign an asset to an asset group. It also allows you to manipulate the assets that are learned from one of the VA vendors.

The **Asset Sources** feature on **Receiver Properties** allows you to retrieve data from your **Active Directory**, if you have one. Once this process is completed, you can filter event data by selecting the retrieved users or groups in the **Source User** and **Destination User** view query filter fields. This improves your ability to provide compliance data for requirements like PCI. An ESM can have only one asset source. Receivers can have multiple asset sources.

If two asset discovery sources find the same asset, the discovery method with the highest priority adds the asset it discovered to the table. If two discovery sources have the same priority, the last one that discovers the asset takes priority over the first.

See also

[Add asset source on page 88](#)

Add asset source

To retrieve data from an **Active Directory**, you must configure a Receiver.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **Receiver Properties**, then click **Asset Sources**.
- 2 Click **Add**, then fill in the information requested.
- 3 Click **OK**, then click **Write** on the **Asset Sources** page.

See also

[Receiver asset sources on page 88](#)

Enterprise Log Search (ELS) settings

Enterprise Log Search (ELS) retains uncompressed log data for specific durations, speeding your ability to search the ELS data quickly from the ESM dashboard.

Before you configure ELS, identify the following information:

- **Storage devices** - Retaining uncompressed data requires additional storage space. Work with your team to determine the appropriate storage requirements for your environment, such as additional hard drives or network storage.
- **Retention policies** - Determine how long you want to retain specific uncompressed data on the ELS device. You can add up to six retention policies with durations in years (365 days), quarters (90 days), or months (30 days).
- **Data sources** - Identify which data sources to associate with the ELS. You can associate a data source with an ELS or an ELM but not with both.

See also

[Configure ELS on page 89](#)

[Search ELS data on page 90](#)



Configure ELS

To search ELS log data, add ELS devices to the console, set up ELS storage and retention policies, and associate data sources with specific retention policies.

Before you begin


Set up and install virtual or physical devices.

Task

- 1 Click , then click **Configuration**.
- 2 Add ELS devices to the console.
 - a On the actions toolbar, click , then select **McAfee Enterprise Log Search**. Click **Next**.
 - b Enter a unique **Device Name**, then click **Next**.
 - c Enter the target IP address or URL, target SSH port number, and Network Time Protocol (NTP) settings for the device. Click **Next**.
 - d Enter a password for this device, then click **Next**.
- 3 Set up storage.




Retaining uncompressed data speeds the ELS search capabilities. But, it requires additional storage space, such as hard drives or network storage.

- a Select **ELS**, click , then click **Data Storage**.
- b If using iSCSI, DAS, SAN, or virtual local drives, fill in the information in the top grid.
- c If using SAN, virtual local, NFS, iSCSI, or CIFS, click **Add** in the lower grid.
- d Enter the correct parameters and click **OK**.

4 Add retention policies (limited to no more than six).



To search ELS log data, you must have at least one retention policy. The system sets the first retention policy created as the default. If only one policy exists, you can change it but you cannot delete it. The ELS cannot accept data older than six months before when you create the first retention policy.

- a Select **ELS**, click , then click **Retention Policies**.
- b Click **Add**.
- c Specify the name and duration of the retention policy and click **OK**.




The system stores duration in days. You can set up a duration in years (365 days), quarters (90 days), or months (30 days).

5 Associate data sources with retention policies.



You can associate a data source with either an ELS or ELM but not with both.

- a Select the data source device (such as a Receiver) and click .
- b Click **Data Sources**.
- c In the **Logging** column, choose the relevant checkbox to display the **Log Data Options** screen.
- d Select the retention policy you want to associate with this data source and click **OK**.

See also

[Enterprise Log Search \(ELS\) settings on page 88](#)

[Search ELS data on page 90](#)



Search ELS data

From the ESM dashboard, quickly search uncompressed log data for specific time periods.

Before you begin

Configure ELS.

Task

- On the dashboard, click  and select **ELS Search**.
 - In the **Filter** bar, enter the information you want to find. Click  to begin the search.
 - Click **Search Settings** to create an advanced search.
 - Click **Search History** to view and rerun previous searches.

See also

[Enterprise Log Search \(ELS\) settings on page 88](#)

[Configure ELS on page 89](#)

Enterprise Log Manager (ELM) settings

ELM supports storing, managing, accessing, and reporting on log data.

The data received by ELM is organized in storage pools, each composed of storage devices. A retention time is associated with each storage pool and the data is retained in the pool for the period specified. Government, industry, and corporate regulations require that logs be stored for different periods of time.

You can set up search and integrity-check jobs on the ELM. Each of these jobs accesses the stored logs and retrieves or checks the data that you define in the job. You can then view the results and export the information.

To configure an ELM, you must know:

- Sources that are storing logs on the ELM
- Required storage pools and their data retention times
- Storage devices that are required to store the data

Generally, you know the sources that store logs on the ELM and the storage pools that are required. What is unknown is the necessary storage devices that store the data. The best approach to addressing this uncertainty is:

- 1 Make a conservative estimate of the storage requirements.



As of 9.0.0, ELM storage pools require 10% of the allocated space for mirroring overhead. Make sure to take this 10% into account when calculating the required space.

- 2 Configure ELM storage devices to meet the estimated requirements.
- 3 Review logs on the ELM for a short period.
- 4 Use ELM storage statistics information to change the storage device configurations to accommodate the actual data storage requirements.

Preparing to store data on the ELM

You must take several steps to configure an ELM to store data.

Step	Action	Description
1	Define data retention times	Based on ELM installation requirements, define the number of different data retention times needed. These are common data retention times: <ul style="list-style-type: none">• SOX – 7 years• PCI – 1 year• GLBA – 6 years• EU DR Directive – 2 years• Basel II – 7 years• HIPAA – 6 or 7 years• NERC – 3 years• FISMA – 3 years
2	Define sources of log data	The goal is to define all sources of logs that are stored on the ELM and estimate the average log byte size and logs generated per day for each. This only needs to be an estimate. It might be easier to estimate the average log byte size and logs generated per day for types of sources then estimate the number of sources for each type. The next step requires associating each source with a retention time defined in Step 1. Make sure to take that into consideration when estimating source types (for example, SOX Firewall, PCI DEM).
3	Define storage pools	Based on ELM installation requirements, associate each source of logs, or source, with a data retention time, defining the set of storage pools required for the ELM installation.

Step	Action	Description
4	Estimate storage pool size requirements	<p>For each storage pool, estimate its storage requirements using one of the following equations:</p> <ul style="list-style-type: none"> Using individual sources: $IRSGB = 0.1 * (DRTD * SUM(DSAB * DSALPD)) / (1024 * 1024 * 1024)$ <p>Where</p> <p>IRSGB= Initial required storage in gigabytes</p> <p>DRTD = Data retention time in days</p> <p>SUM() = The sum for all data sources</p> <p>DSAB = Data source average bytes per log</p> <p>DSALPD = Data source average logs per day</p> Using source types: $IRSGB = 0.1 * (DRTD * SUM(NDS * DSTAB * DSTALPD)) / (1024 * 1024 * 1024)$ <p>Where</p> <p>IRSGB= Initial required storage in gigabytes</p> <p>DRTD = Data retention time in days</p> <p>NDS = Number of data sources of a data source type</p> <p>SUM() = The sum for all data source types</p> <p>DSTAB = Data source type average bytes per log</p> <p>DSTALPD = Data source type average logs per day</p>
5	Create initial storage devices	Create one or more ELM storage devices so they are large enough to store each IRSGB worth of data (see <i>Add a storage device</i>).
6	Create storage pools	<p>For each storage pool you defined in Step 3, create an ELM storage pool using the following:</p> <ul style="list-style-type: none"> The associated retention time from Step 1 The associated IRSGB values from Step 4 The associated storage devices from Step 5 (see <i>Add a storage pool</i>)
7	Start logging data	Configure sources to send their logs to the ELM, and let them do so for one or two days.
8	Refine storage pool size requirement estimates	<p>For each storage pool created in Step 6, refine its storage requirement estimate using the following equation:</p> $RSGB = 1.1 * DRTD * SPABRPD / (1024 * 1024 * 1024)$ <p>Where</p> <p>RSGB = Required storage in gigabytes</p> <p>DRTD = Data retention time in days</p> <p>SPABRPD = Storage pool's daily "Avg. byte rates" value from its Statistical Report</p>
9	Change or create storage devices	For each RSGB value from Step 8, change or create ELM storage devices so that they are large enough to store RSGB worth of data.
10	Change storage pools	If needed, change each storage pool created in Step 6 by adding storage devices created in Step 9, or increase existing storage device allocation.

Setting up ELM storage

To store logs, the ELM must have access to at least one storage device.

The storage requirement for an ELM installation is a function of the number of data sources, their logging characteristics, and their data retention time requirements. The storage requirement varies over time because all are likely to change during the life of an ELM installation.

For details regarding estimating and adjusting the storage requirements for your system, see *ELM settings*.

ELM storage terminology

Review these terms to work with ELM storage:

- **Storage Device** — A data storage device accessible to an ELM. Some ELM models offer an onboard storage device, some offer a SAN connection capability, and some both. All ELM models offer an NAS connection capability.
- **Storage Allocation** — A specific amount of data storage on a specific storage device (for example, 1 TB on an NAS storage device).
- **Data Retention Time** — The amount of time a log is stored.
- **Storage Pool** — One or more storage allocations, which together specify a total amount of storage, coupled with a data retention time that specifies the maximum number of days a log is to be stored.
- **Log Source** — Any source of logs that an ELM stores.

ELM storage device types

When you are adding a storage device to an ELM, you must select the type of device it is. There are a few things to keep in mind when you are adding or editing the device.

Device type	Details
NFS	To edit the remote mount point of the storage device containing the ELM Management Database, use the Migrate DB option to move the database to a different storage device (see <i>Migrate ELM database</i>). You can then safely change the remote mount point field and move the database back to the updated storage device.
CIFS	<ul style="list-style-type: none">• Using the CIFS share type with Samba server versions later than 3.2 can result in data loss.• When connecting to a CIFS share, don't use commas in your password.• If you are using a Windows 7 computer as a CIFS share, see <i>Disable HomeGroup file sharing</i>.
iSCSI	<ul style="list-style-type: none">• When connecting to an iSCSI share, don't use commas in your password.• Attempting to attach multiple devices to one IQN can cause data loss and other configuration problems.
SAN	The SAN option is available only if there is a SAN card installed on the ELM and there are SAN volumes available.
Virtual Local	This option is available only if a virtual local device has been added to the virtual ELM. You must format the device prior to using it for storage (see <i>Set up virtual local drive to store data</i>).

Disable HomeGroup file sharing

Windows 7 requires you to use HomeGroup file sharing, which works with other Windows 7 computers but not with Samba. To use a Windows 7 computer as a CIFS share, you must disable HomeGroup file sharing.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Open the Windows 7 **Control Panel**, then select **Network and Sharing Center**.
- 2 Click **Change advanced sharing settings**.
- 3 Click **Home or Work** profile and make sure it is labeled as your current profile.
- 4 Turn on network discovery, file and printer sharing, and public folder.
- 5 Go to the folder you want to share using CIFS (try the public folder first) and right click it.
- 6 Select **Properties**, then click the **Sharing** tab.
- 7 Click **Advanced sharing**, then select **Share this folder**.
- 8 (Optional) Change the share name and click **Permissions**.
Make sure you have permissions set as you want (a checkmark in Change = writeable). If you've enabled password-protected shares, you'll have to tweak settings here to make sure that your Ubuntu user is included for permission.

Add a storage device to link to a storage pool

To add a storage device to the list of storage locations, you must define its parameters.



When editing a storage device, you can increase the size, but you can't reduce it. A device can't be deleted if it's storing data.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **Storage Pools**.
- 2 Click **Add** next to the top table.
- 3 On the **Add Storage Device** page, fill in the requested information.
- 4 Click **OK** to save the settings.

The device is added to the list of available ELM storage devices.

You can edit or delete storage devices from the table on the **Storage Pools** page.



Table 3-40 Option definitions

Option	Definition
Device Type	Select the type of storage device. Migrating the ELM database requires a minimum of 506 GB of free disk space. See <i>ELM storage device types</i> in <i>Setting up ELM storage</i> for details about each type.
Name	Type a name for the storage device.
Max size	Select the maximum amount of storage space that you want to allocate on this device. <ul style="list-style-type: none"> When adding a remote storage device to the ELM, Max size defaults to 4 GB. One percent of the storage space is reserved for management of the remote storage. When adding a virtual local storage device, Max size defaults to the total storage capacity of the device. Six GB of the storage space is reserved for management of the virtual storage. You can't adjust this field.

Table 3-40 Option definitions *(continued)*

Option	Definition
IP Address, Remote Mount Point, Remote Path	Type this information for the NFS device.
IP Address, Remote Share Name, Path, Username, Password	Type this information for the CIFS device.
iSCSI Device	Select the device that you added (see <i>Add an iSCSI device</i>).
iSCSI IQN	Select the IQN.
SAN	Select the SAN volume that you added (see <i>Format a SAN storage device to store ELM data</i>).
Virtual Local Volume	Select the virtual local storage device. This option is only available when the device type is Virtual Local .

Table 3-41 Option definitions

Option	Definition
Data Storage Devices	Select the device you want to add. If the device you want to select isn't listed, you must add it (see <i>Add a storage device</i>). <div>  A device can be assigned to more than one pool at a time. </div>
Storage space	Select the maximum amount of space on this device for storing data. <div>  Ten percent of the storage space is used for overhead. If you select 4GB in the storage space field, 3.6GB of the 4 is actually available to store data. </div>
Mirrored Data Storage Device	If you want the data on this storage device mirrored on another device, select the second storage device (see <i>Add mirrored ELM data storage</i>).

Add or edit a storage pool

A storage pool includes one or more storage allocations and a data retention time. To define where ELM logs are stored and how long they must be retained, add them to the ELM.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **Storage Pool**.
- 2 Click **Add** or **Edit** next to the bottom table, then fill in or change the information requested.
- 3 Click **OK**.

You can edit the parameters after they are saved, and you can delete a storage pool as long as it, and the devices allocated to it, isn't storing data.


Table 3-42 Option definitions

Option	Definition
Add storage device	Add a storage device to be used with a storage pool for data retention.
Edit storage device	Change the settings of an existing storage device.
Delete storage device	Delete a storage device from the system.
Add storage pool	Add a storage pool to hold a maximum amount of data for a specific period.

Table 3-42 Option definitions *(continued)*

Option	Definition
Edit storage pool	Change the storage pool name or the retention period of an existing storage pool. Add space to a pool from a defined storage device.
Delete storage pool	Delete a storage pool from the system.
Rebuild	Repair mirrored storage pools that have lost connection with one of their storage devices. This option is only available when there is a problem with a mirrored storage pool.
Reduce size	Reduce the amount of space defined for each allocation.
Refresh	Update the information in the tables.

Table 3-43 Option definitions

Option	Definition
Storage Pool Name	Type a name for this pool.
Data Retention Time	Select the amount of time you want to store this data.
Data Storage Devices that are linked	<p>Lists the devices linked to this storage pool. To add devices, click Add.</p> <div>  <p>Mirrored allocations that use network protocols (CIFS, NFS, and iSCSI) require specific configurations to work reliably such as being on the same switch and having a very low latency. Recommended network specifications are:</p> <ul style="list-style-type: none"> • Total latency (server plus network) — 10 ms • Total throughput (server plus network) — 20 Mb/sec <p>Mirroring assumes 100% availability of the share.</p> </div>
Enabled column	Select the devices you want to enable to store data. Mirrored storage devices are disabled until the mirroring process is complete.

Move a storage pool


You can move a storage pool from one device to another.

Before you begin

Set up the storage device you want to move the storage pool to as a mirror of the device currently holding the pool (see *Add mirrored ELM data storage*).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the ELM device holding the storage pool, then click the **Properties** icon .
- 2 Click **Storage Pools**.
- 3 In the **Storage Pools** table, click the mirrored devices listed under the pool to be moved.
- 4 Click **Edit**, and from the **Data Storage Devices** drop-down list, select the device that mirrors the storage pool to be moved.

It is now the main data storage device.
- 5 To mirror the new data storage device, select a device from the **Mirrored Data Storage Device** drop-down list, then click **OK**.

Reduce storage allocation size

If a storage device is full due to space allocated for storage pools, you might need to reduce the amount of space defined for each allocation. This might be necessary to allocate space on this device for more storage pools.



If the allocation size reduction affects data, the data is moved to other allocations in the pool if the space is available. If it is not available, the oldest data is deleted.

Task


For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select **ELM Properties**, then click **Storage Pool**.
- 2 On the bottom table, select the pool to be reduced, then click **Reduce Size**.
- 3 Enter the amount you want to reduce the storage by, then click **OK**.

Mirroring ELM data storage


You can set up a second ELM storage device to mirror the data collected on the main device.

If the main device goes down for any reason, the backup device continues storing the data as it comes in. When the main device comes back on line, it automatically syncs with the backup, then resumes storing the data as it arrives. If the main device goes down permanently, you can reassign the backup to become the main on the ESM, then designate a different device to mirror it.

When either of the devices go down, a health status flag  appears next to the ELM device on the system navigation tree.

A mirrored storage pool might lose connection with its storage device. The loss can be due to:

- The file server or the network between the ELM and the file server has failed.
- The file server or network is shut down for maintenance.
- An allocation file is accidentally deleted.

When there is a problem with the mirror, the storage devices show a warning icon  in the **Storage Pools** table. You can then use the **Rebuild** function to repair it.

Add mirrored ELM data storage

Any storage device added to the list of available devices that has the needed space, can be used to mirror the data saved on an ELM storage device.

Before you begin

Add the two devices you want to use to mirror each other to the ESM.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select **ELM Properties**, then click **Storage Pools**.
- 2 Click **Add** next to the bottom table

- 3 On the **Add Storage Pool** page, enter the information requested, then click **Add** to select the storage device and mirroring device.



A device can be assigned to more than one pool at a time.

- 4 Click **OK** twice.

Rebuild a mirrored storage pool

If a mirrored storage pool loses connection with its storage devices, you can use the **Rebuild** function to repair it.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **Storage Pool**.
- 2 Hover over the mirrored devices that are showing a warning icon.

A tool tip informs you that the ELM allocation is rebuilding or that the mirrored device needs to be rebuilt.

- 3 To rebuild the mirrored devices, click on the devices, then click **Rebuild**.


When the process is complete, you are notified that the allocation rebuilt successfully.

Disable a mirroring device

To stop using a device as a storage pool mirroring device, you must select a different device to replace it or select **None**.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the ELM currently holding the mirroring storage pool in the system navigation tree, then click the **Properties** icon .
- 2 Click **Storage Pools**, then select the mirrored devices in the **Storage Pool** table and click **Edit**.
- 3 Do one of the following:
 - If the device selected in the **Mirrored Data Storage Device** field is the one you want to disable, click the drop-down arrow in that field and select a different device to mirror the data storage device or select **None**.
 - If the device selected in the **Data Storage Device** field is the one you want to disable, click the drop-down arrow in that field and select a different device to act as the data storage device.
- 4 Click **OK** to save the changes.

If the device is no longer a mirroring device, it still appears in the **Storage Device** table.

Set up external data storage

There are four types of external storage that can be set up to store ELM data: iSCSI, SAN, DAS, and virtual local. When you connect these external storage types to the ELM, you can set them up to store data from the ELM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **Data Storage**.
The system returns all available storage devices on the appropriate tabs.

- 2 Click the **iSCSI**, **SAN**, **DAS**, or **Virtual Local** tab, then follow the required steps.
- 3 Click **Apply** or **OK**.

Add an iSCSI device

To use an iSCSI device for ELM storage, you must configure connections to the device.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **Data Storage**.
- 2 On the **iSCSI** tab, click **Add**.
- 3 Enter the information requested, then click **OK**.

If the connection is successful, the device and its IQNs are added to the **iSCSI Configuration** list and the **Device Type** list on the **Add Storage Device** page.



Once an IQN begins storing ELM logs, the iSCSI target can't be deleted. Due to this limitation, make sure to set up your iSCSI target with sufficient space for ELM storage.

- 4 Before using an IQN for ELM storage, select it on the list, then click **Format**.
- 5 To check its status as it is formatting, click **Check Status**.
- 6 To discover or rediscover the IQNs, click the iSCSI device, then click **Discover**.



Attempts to assign more than one device to an IQN can result in data loss.

Table 3-44 Option definitions

Option	Definition
Add	Add the parameters needed to connect to the iSCSI device.
Delete	Delete the selected iSCSI connection.
Discover	Discover or rediscover the IQNs for the selected iSCSI.
Check Status	Check the status of IQN as it is formatting.
Format	Format the selected IQN prior to using it for ELM storage.

Table 3-45 Option definitions

Option	Definition
Name	Type the name of the iSCSI device.
IP Address	Type the IP address for the iSCSI device
Port	Select the port for the iSCSI device.

Format a SAN storage device to store ELM data

If you have a SAN card in your system, you can use it to store ELM data.

Before you begin

Install a SAN card in your system (see *Install the qLogic 2460 or 2562 SAN adapters* in the McAfee ESM Installation Guide, or contact McAfee support).

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **Data Storage**.
- 2 Click the **SAN** tab, then check the status of the SAN volumes that were detected.
 - **Format required** — The volume must be formatted and doesn't appear on the list of available volumes on the **Add Storage Device** page.
 - **Formatting** — The volume is in the process of being formatted and doesn't appear on the list of available volumes.
 - **Ready** — The volume is formatted and has a recognizable file system. These volumes can be used to store ELM data.
- 3 If a volume is not formatted and you want it to store data, click it, then click **Format**.



When you format a volume, all stored data is deleted.

- 4 To check if formatting is complete, click **Refresh**.

If formatting is completed, the status changes to **Ready**.
 - 5 To view the details of a volume at the bottom of the page, click the volume.
- You can now set up the formatted SAN volume as a storage device for ELM storage.

Assign a DAS device to store data

You can assign available DAS devices to store ELM data.

Before you begin

Set up DAS devices.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the ELM you will assign the DAS device to, then click the **Properties** icon



On an all-in-one device, you can assign the DAS to the ESM by selecting the ESM, then clicking the **Properties** icon.

- 2 Click **Data Storage**, then click the **DAS** tab.

The **DAS** table lists the devices that are available for storage.
- 3 On the table, click one of the devices that has not been assigned to store ELM or ESM data.
- 4 Click **Assign**, then click **Yes** on the warning page.



Once you assign a device, you can't change it.

The ELM restarts.

Set up virtual local drive to store data

Detect and format a virtual storage device on the virtual ELM. It can then be used for database migration and storage pools.

Before you begin

Add a virtual local storage device to the virtual ELM from its virtual environment. To add the storage, see the documentation for the virtual machine environment.

Supported virtual environments

- VMware
- KVM
- Amazon Web Service

Supported drive formats

- SCSI
- SATA



IDE is not supported.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the virtual ELM, click the **Properties** icon , then click **Data Storage**.

A loading icon appears while the system returns all available storage devices. If the system has a redundant ESM, the devices are returned under the **Redundant** tab.



Root and boot partitions are not available as viable storage options.

- 2 Click the **Virtual Local** tab, then select a device from the list of available virtual devices.



The **Virtual Local** tab is only available if the system detects virtual storage.

- 3 If the **Status** column says **Format required**, click **Format** to format the device with ext4 file format.

The status changes to **Ready**.

You can now use this device for database migration and storage pools.

ELM redundancy

You can provide redundancy for your logging by adding a standby ELM to the current standalone ELM on your system.

To enable redundancy, define the IP addresses and other network information on two ELMs (see *Set up ELM redundancy*). The standby ELM must have storage devices with enough combined space to match the storage on the active ELM. Once they are set up, the configuration on both ELMs is synchronized, and the standby ELM maintains the synchronization of data between both devices.

There are several actions you perform when working with ELM redundancy: switch over, return to service, suspend, remove, and view status. All actions are available on the **ELM Properties | ELM Redundancy** page.

Switch over

If the primary ELM goes down or needs to be replaced, select **Switch ELM**. The standby ELM becomes active and the system associates all logging devices to it. Logging and configuration actions are locked during the switch-over process.

Return to service

If the standby ELM goes down, you must return it to service when it is brought back up. If no changes to configuration files are detected, redundancy continues as before. If differences are detected in the files, redundancy continues for the storage pools that do not have problems, but an error status is returned, that one or more pools are out of configuration. You must fix these pools manually.

If the standby ELM has been replaced or reconfigured, the system detects it and prompts you to re-key the standby ELM. The active ELM then syncs all configuration files to the standby, and redundancy continues as before.

Suspend

You can suspend communication with the standby ELM if it is down or is going to be down for any reason. All communication stops and error notifications for redundancy are masked. When the standby ELM is brought back up, follow the return to service process.

Disable redundancy on the ELM

You can disable ELM redundancy by selecting **Remove**. The active ELM saves a copy of the redundancy configuration files. If this backup file is found when enabling ELM redundancy, you are asked if you want to restore the saved configuration files.

View status

You can view details on the state of data synchronization between the active and standby ELM by selecting **Status**.

See also

[Set up ELM redundancy on page 102](#)

Set up ELM redundancy


If you have a standalone ELM device on your system, you can provide redundancy for logging by adding a standby ELM.

Before you begin

You must have a standalone ELM installed (see *McAfee Enterprise Security Manager 9.5.0 Installation Guide*) and added to the ESM console (see *Add devices to the ESM console*). You must also have a standby ELM installed but not added to the console. Ensure that there is no data on the standby ELM. Contact McAfee support if you need to perform a factory reset.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, click the ELM, then click the **Properties** icon .
- 2 On the **ELM Properties** page, click **ELM Redundancy**, then click **Enable**.
- 3 Type the IP address and password for the standby ELM, then click **OK**.

- 4 On the **ELM Properties** page, click **Storage Pools**, and verify that the **Active** tab is selected.
- 5 Add storage devices to the active ELM (see *Add a storage device to link to a storage pool*).
- 6 Click the **Standby** tab, then add storage devices that have enough combined space to match the storage on the active ELM.
- 7 Add one or more storage pools to each ELM (see *Add or edit a storage pool*).

The configuration on both ELMs is now synchronized and the standby ELM maintains the synchronization of data between both devices.

Table 3-46 Option definitions

Option	Definition
	Available only when ELM redundancy is not enabled.
Enable	Click, then add standby ELM data to activate ELM redundancy.
	Available only when ELM redundancy is enabled
Remove	Click to disable redundancy on the ELM.
Switch ELMs	Click to switch the ELMs so the standby ELM becomes the primary ELM. The system associates all logging devices to it. Logging and configuration actions are locked during the switch-over process.
Suspend	Click to suspend communication with the standby ELM if it is experiencing problems. All communication stops and error notifications for redundancy are masked. When you bring the standby ELM back up, click Return to Service .
Status	Click to view details on the state of data synchronization between the active and standby ELM.
Return to service	<p>Click to return a repaired or replaced standby ELM to service. If the system brings the ELM back up and detects no changes to the configuration files, redundancy continues as before. If the system does detect differences, the redundancy process continues for the storage pools without problems, and you are informed that one or more pools are out of configuration. Fix these pools manually.</p> <p>If you replace or reconfigure the standby ELM, the system detects it and prompts you to re-key it. The active ELM then syncs all configuration files to the standby ELM and the redundancy process continues as before.</p>

See also

[ELM redundancy on page 101](#)

Managing ELM compression

Compress the data coming in to the ELM to save disk space or process more logs per second.

The three options are **Low** (default), **Medium**, and **High**. This table shows details about each level.

Level	Compression rate	Percentage of maximum compression	Percentage of maximum logs processed per second
Low	14:1	72%	100%
Medium	17:1	87%	75%
High	20:1	100%	50%



Actual compression rates vary depending on the content of the logs.

- If you are more concerned with saving disk space and less concerned with the number of logs you can process per second, choose high compression.
- If you are more concerned with processing more logs per second than you are with saving disk space, then choose low compression.

See also

[Set ELM compression on page 104](#)

Set ELM compression

Select the compression level for the data coming into the ELM to save disk space or process more logs.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **ELM Configuration | Compression**.
- 2 Select the ELM compression level, then click **OK**.

You are notified when the level is updated.

Table 3-47 Option definitions

Option	Definition
ELM compression level	Select Low , Medium , or High . See <i>Set ELM Compression</i> for details about each of these settings.

See also

[Managing ELM compression on page 103](#)

Back up and restore ELM

Back up the current settings on ELM devices so you can restore them in case of a system failure or data loss. All configuration settings, including the ELM logging database, are saved. The actual logs that are stored on the ELM are not backed up.

We recommend that you mirror the devices that store the log data on the ELM, and mirror the ELM management database. The mirroring feature provides real-time log data backup.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**.
- 2 Make sure that **ELM Information** is selected, then click **Backup & Restore**.
- 3 Do one of the following:

To...	Do this...
Back up ELM now	Provide the requested information, then click Backup Now .
Back up ELM settings automatically	Select the frequency and provide the information.
Restore backup now	Click Restore Backup Now . The ELM database is restored to the settings from a previous backup.

Table 3-48 Option definitions

Option	Definition
Backup Frequency	To back up the settings automatically, select this option and enter the frequency.
Backup Location	Select the type of share, then enter the information for the remote location where the information is saved.
Connect	Click to test the connection.
Backup Now	Click to back up the data now.
Restore Backup	Click to restore the ELM database to the settings from a previous backup. ELM data storage is not restored.
Restore ELM	Restore the management database and ELM data storage.

Restore ELM management database and log data

To replace an ELM, restore the management database and log data to the new ELM. For this to work, the database and log data must be mirrored.



To restore the data from an old ELM to a new ELM, don't create a new ELM using the **Add Device** wizard.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties** for the ELM that must be replaced.
A warning page lets you know that the system can't locate the ELM.
- 2 Close the warning page, then click **Connection**.
- 3 Enter the IP address for the new ELM, then click **Key Management** | **Key Device**.
You are informed when the new device is keyed successfully.
- 4 Enter the password that you want associated with this device, then click **Next**.
- 5 Click **ELM Information** | **Backup & Restore** | **Restore ELM**.
- 6 Re-sync each device logging to the ELM by clicking **Sync ELM** on the **Properties** | **Configuration** page for each device.

The management database and ELM data storage are restored on the new ELM. This process can take several hours.

Define an alternate storage location



To store ELM management database records in a location not on the ELM, you must define the alternate storage location. You can also select a second device to mirror what is stored.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **ELM Configuration | Migrate DB**.
- 2 Select the storage device and a mirrored device.
- 3 Click **OK**.

Table 3-49 Option definitions

Option	Definition
Gigabytes of space	Set the amount of space to allocate for the management database.
Data Storage Devices	Select the location to store the management database. <div>  If you need to add a device to the list or edit a device that is currently listed, see <i>Add a storage device</i>. </div>
Mirrored Data Storage Device	Select a second storage location to mirror the data storage device. <div>  If you upgrade your system from a version prior to 9.0, the first time you select to mirror any of the existing devices, the process takes an extended amount of time. </div>

See also

[Migrating ELM database on page 106](#)

[Replace an ELM mirrored management database on page 107](#)

View ELM storage usage

Viewing the usage of storage on the ELM can help you make decisions regarding space allocation on the device.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ELM Properties**, then click **ELM Management**.
- 2 Click **View Usage**.

The **Usage Statistics** page opens, showing the statistics for the storage device and pools on the ELM.

- 3 Click **OK**.

Migrating ELM database

The ELM management database stores the records that keep track of the logs sent to the ELM. The amount of disk space that is available on your ELM device to store the management database depends on the model.

When you first add the device, the system verifies if it has enough disk space to store the records. If it doesn't, you are prompted to define an alternate location for management database storage. If the device does have enough disk space but you prefer to save the database in an alternative location, you can use **Migrate DB** on the **ELM Properties** page to set up that location.

Migrate DB can be used at any time. However, if you migrate the management database once it contains records, the ELM session is on hold for several hours until the migration is complete, based on the number of records it contains. We recommend that you define this alternative location when you first set up the ELM device.

See also

[Define an alternate storage location on page 106](#)


[Replace an ELM mirrored management database on page 107](#)

Replace an ELM mirrored management database

If a mirrored management database storage device is having a problem, you might need to replace it.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the ELM device with the management database storage device that's experiencing the problem, then click the **Properties** icon .
- 2 Click **ELM Configuration**, then select **Migrate DB**.
- 3 In the **Data Storage Devices** field, select the device listed in the **Mirrored Data Storage Device** drop-down.
- 4 Select a new device in the **Mirrored Data Storage Device** field or select **None** to stop mirroring.



If the device you want isn't listed on the drop-down list, add the device to the **Storage Device** table first.

See also

[Migrating ELM database on page 106](#)

[Define an alternate storage location on page 106](#)

Retrieving ELM data

To retrieve data from the ELM, you must create search and integrity-check jobs on the **Data** page.

An integrity-check job checks if the files that you define have been altered since they were originally stored. This can alert you to unauthorized modification of critical system or content files. The results of this check show which files were altered. If none of the files were altered, you are notified that the check was successful.

The system is limited to a total of 50 searches and integrity-check jobs at one time. If there are more than 50 on the system, you are informed that your search can't be performed. If you have existing searches on the system, you can delete them so that your new search can be performed. If you do not have existing searches, the system administrator deletes existing searches or integrity-check jobs initiated by other users for your search to be performed.

Once you initiate a search, it continues to run until it is complete or it reaches one of the limits you have set, even if you close the **Data** page. You can return to this screen to check on the status, which is displayed in the **Search Results** table.

See also

[Create a search job on page 108](#)

[Create an integrity-check job on page 108](#)


[View results of a search or integrity check on page 109](#)

[Using regex to query the ELM on page 110](#)

Create a search job

To search ELM for files that match your criteria, you must define a search job on the **Data** page. No fields on this screen are required; but the better you define your search, the more likely you are to retrieve the data you require.

Task

- 1 From the dashboard, click  and select **ELM Search**.
- 2 On the system navigation tree, select **ELM Properties**, then click **Data**.
- 3 On the **Search Logs and Files** tab, fill in the information requested, then click **Search**.

See also

[Retrieving ELM data on page 107](#)

[Create an integrity-check job on page 108](#)

[View results of a search or integrity check on page 109](#)

[Using regex to query the ELM on page 110](#)

Create an integrity-check job

You can check if files were altered since they were originally stored by creating an integrity-check job on the **Data** page. None of the fields on the **Integrity Check** tab are required; however, the better you are able to define your search, the more likely you are to verify the integrity of the data you require in the least amount of time.

Task


- 1 From the dashboard, click  and select **ELM Search**.
- 2 On the system navigation tree, select **ELM Properties**, then click **Data**.
- 3 Click the **Integrity Check** tab, make the requested selections, then click **Search**.

Table 3-50 Option definitions




Option	Definition
Logs, Files	Select whether you want to check ELM logs, ELM files, or both.
Time Frame	Select the time frame of the data to be checked.
Device	Click the filter icon  and select the devices to be checked.
Device Type	Click the filter icon  and select the types of devices to be checked.
Filename	If you want a specific file to be checked, type the name.
Filename is case insensitive	If you want the file name to be case insensitive, select this option.
Limit search time	To limit the time to be spent on the search, select the number of hours. If you select zero, there is no time limit.
Max result file size	To limit the size of the result file, select the maximum number of MB.
Open field	Type a descriptive name for this job.
Search	Click to start the job.

Table 3-50 Option definitions *(continued)*

Option	Definition
Search Results	<p>View the list of completed jobs. The status of each job will be indicated in the State column.</p> <ul style="list-style-type: none">• Waiting — The job has not begun to process yet. The system can only process 10 jobs at a time and it processes them in the order received.• Executing — The job is currently in progress.• Complete — The job is finished. You can view the results or download the export.• Limit Reached — The time or size limit was reached. You can view results, but they are incomplete.
View	View the results of the selected job.
Export	Export the results of the selected job.
	 All ELM searches can be lost if you remove more than one extra VM drive from the ESM at one time. To avoid losing the results, export the ELM search results.
Delete	Mark the selected job for deletion.
Reload Search	Perform the selected job again.

See also

[Retrieving ELM data on page 107](#)

[Create a search job on page 108](#)

[View results of a search or integrity check on page 109](#)

[Using regex to query the ELM on page 110](#)


View results of a search or integrity check

When a search or integrity check job is completed, you can view the results.

Before you begin

Run a search or integrity check job that produces results.

Task


- 1 From the dashboard, click  and select **ELM Search**.
- 2 Click **Data**, then select the **Search Logs and Files** or **Integrity Check** tab.
- 3 Highlight the job that you want to view on the **Search Results** table, then click **View**.

The **ELM search results** page displays the results of the job.



All ELM searches can be lost if you remove more than one extra VM drive from the ESM at one time. To avoid losing the results, export the ELM search results.

Table 3-51 Option definitions

Option	Definition
Parameters	View the parameters that were used to generate the results on the page.
Export	Export a summary of the data. <div>  All ELM searches can be lost if you remove more than one extra VM drive from the ESM at one time. To avoid losing the results, export the ELM search results. </div>
Download File	To save the data for specific files, highlight the files on the table, then click this option.
Value	View the value for the selected item on the list.

See also

[Retrieving ELM data on page 107](#)

[Create a search job on page 108](#)

[Create an integrity-check job on page 108](#)

[Using regex to query the ELM on page 110](#)

Using regex to query the ELM

The ELM uses bloom indexes to optimize queries. While most Perl Compatible Regular Expressions (PCRE) can be used for ELM searches, not every PCRE can be optimized to use the bloom.

The bloom regex optimizer performs pre-tuning to provide optimal searches, but you can obtain even better performance from your queries by keeping a few things in mind.

- You can only use mandatory parts of the regular expression for bloom filtering. The bloom filter only uses substrings in the regular expression that exist in every matching string. The one exception is that you can use a one-level deep OR grouping such as `(seth|matt|scott|steve)`.
- You can't use mandatory parts of a regular expression that are shorter than four characters. For example, `seth.*grover` uses `seth` and `grover` with the bloom, but `tom.*wilson` only uses `wilson` because `tom` is too short.
- OR groupings that contain non-constant substrings or a substring that is too-short can't be used. For example, `(start|\w\d+|ending)` can't be used because the middle item in the OR list is not a constant that can be searched for in the bloom. As another example, `(seth|tom|steve)` can't be used because `tom` is too short; but `(seth|matt|steve)` can be used.

The regex-to-bloom query is run by the optimizer process for the database. That optimizer deconstructs the regex and finds the mandatory constant substrings.

As an example, the original regular expression is:

```
\\|\\| (626|629|4725|4722) \\|\\| . * \\|\\| (bbphk) \\|\\|
```

The only part that the bloom uses from this expression is `bbphk`. This change reduces the search set from over a million files down to 20,000.

The regular expression can be further optimized in the following way:

```
(\\|\\| 626\\|\\|\\|\\|\\| 629\\|\\|\\|\\|\\| 4725\\|\\|\\|\\|\\| 4722\\|\\|) . * \\|\\| bbphk \\|\\|
```

In this example, the `\\|\\|` has been moved from before and after the first group to the front and back of each element in the group, which does two things:

- It allows the pipe characters to be included.
- It makes the elements in the first group, which were ignored because they were only three characters, longer than four characters so they can be used.

In addition, the parentheses around `bbphk` have been removed as they were not needed and indicated to the bloom filter that this is a new subgroup. Performing these types of manual adjustments to the regular expression can effectively reduce the search even further to only about 2,000 files.

See also

[Retrieving ELM data on page 107](#)

[Create a search job on page 108](#)

[Create an integrity-check job on page 108](#)

[View results of a search or integrity check on page 109](#)

Advanced Correlation Engine (ACE) settings

McAfee Advanced Correlation Engine (ACE) identifies and scores threat events in real time, using both rule- and risk-based logic.

Identify what you value (users or groups, applications, specific servers, or subnets) and ACE alerts you if the asset is threatened. Audit trails and historical replays support forensics, compliance, and rule tuning.

Configure ACE using real-time or historical modes:

- **Real-time mode** — analyzes events as they are collected for immediate threat and risk detection.
- **Historical mode** — replays available data collected through either or both correlation engines for historical threat and risk detection. When ACE discovers new zero-day attacks, it determines whether your organization was exposed to that attack in the past, for *subzero day* threat detection.

ACE devices supplement the existing event correlation capabilities for ESM by providing two dedicated correlation engines. Configure each ACE device with its own policy, connection, event and log retrieval settings, and risk managers.

- **Risk correlation** — generates a risk score using rule-less correlation. Rule-based correlation only detects known threat patterns, requiring constant signature tuning and updates to be effective. Rule-less correlation replaces detection signatures with a one-time configuration: Identify what is important to your business (such as a particular service or application, a group of users, or specific types of data). **Risk Correlation** then tracks all activity related to those items, building a dynamic risk score that raises or lowers based on real-time activity.

When a risk score exceeds a certain threshold, ACE generates an event and alerts you to growing threat conditions. Or, the traditional rule-based correlation engine can use the event as a condition of a larger incident. ACE maintains a complete audit trail of risk scores for full analysis and investigation of threat conditions over time.

- **Rule-based correlation** — detects threats using traditional rule-based event correlation to analyze collected information in real time. ACE correlates all logs, events, and network flows with contextual information, such as identity, roles, vulnerabilities, and more—to detect patterns indicative of a larger threat.

Event Receivers support network-wide, rule-based correlation. ACE complements this capability with a dedicated processing resource that correlates larger volumes of data, either supplementing existing correlation reports or off-loading them completely.

Configure each ACE device with its own policy, connection, event and log retrieval settings, and risk managers.

Select ACE data type

ESM collects both event and flow data. Select which data to send to the ACE. Default is event data only.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ACE Properties**, then click **ACE Configuration**.
- 2 Click **Data**, then select **Event Data**, **Flow Data**, or both.
- 3 Click **OK**.

Add a correlation manager

To use rule or risk correlation, you must add rule or risk correlation managers.

Before you begin

There must be an ACE device on the ESM (see *Add devices to the ESM console*).

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ACE Properties**.
- 2 Click **Correlation Management**, then click **Add**.
- 3 Select the type of manager that you want to create, then click **OK**.



See *Advanced Correlation Engine (ACE) settings* for information about the types of managers.

- 4 Enter the requested information, then click **Finish**.

Add a risk correlation manager

Add managers to help calculate the levels of risk for the fields that you designate.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **ACE Properties**, then click **Risk Correlation Management**.
- 2 Click **Add**, then fill in the information requested on each tab.
- 3 Click **Finish**, then click **Write** to write the managers to the device.

Table 3-52 Option definitions

Option	Definition
Table	View the existing correlation managers on the ACE.
Add	Add a new correlation manager.
Edit	Edit the selected correlation manager.
Remove	Delete the selected manager.
Enabled	Enable the selected manager.
Maximum number of field combinations	Select the maximum number of field combinations a manager can have. This limit helps with processing time on the system. This number is in the thousands.
Write	Write the correlation managers to the device.

Table 3-53 Option definitions








Tab	Option	Definition
Main	Name	Type a name for the manager.
	Enable	Deselect to disable the manager.
	Use Event Data, Use Flow Data	Select either or both to indicate the type of data that you want to use. <div>  If you select Use Flow Data, you must also go to ACE Properties ACE Configuration Data and select Flow Data. </div>
	Logging, Storage Pools	Select Logging to save the logs on the ELM. Select the storage pool on the ELM where you want the logs saved. <div>  If you haven't selected an ELM to store the data, see <i>Set default logging pool</i>. </div>
	Zone	If you want the data to be assigned to a zone, select it from the drop-down list (see <i>Zone management</i>).
	Time Order Tolerance	(Rule Correlation only) Select the amount of time that the rule correlation allows for events to be out of order. For example, if the setting is 60 minutes, an event that is 59 minutes late is still used.
Fields	Field	Select the fields that this manager uses to correlate events (maximum of five per manager).
	Percentage	Select the percentage that you want each field to have. They must add up to the overall score of 100%. <div>  Risk updates, when below 100% critical, report their criticality in terms of what you have defined as <i>FYI</i>, <i>Minor</i>, <i>Warning</i>, <i>Major</i>, and <i>Critical</i> (see Thresholds tab). For example, if your concept of FYI is 50% of the critical value when the risk is at 50% of critical, the severity is actually 20 rather than 50. </div>

Table 3-53 Option definitions *(continued)*

Tab	Option	Definition
	Correlate	<p>Select if you don't want a field to be used to determine uniqueness. Due to the memory required, correlating against multiple high cardinality fields is not recommended.</p> <p> The number of risk lines being generated depends on the number of unique combinations of all correlated fields.</p>
Thresholds	Top section	Set the score thresholds for an event to trigger for each criticality level.
	Bottom section	Set the rate for the score to decay. The default setting is that every 120 seconds that a score is in a bucket, it decays by 10 percent until it reaches a score of 5. The bucket for the unique field values is then deleted.
Filters	Logic AND, Logic OR	Set up the framework for the filters using logic elements (see <i>Logic elements</i>).
	Filter Fields Component	<p>Drag and drop the Match Component icon  onto a logic element, then complete the Add Filter Field page.</p> <p> To edit the conditions of a component after it has been added to a logic element, click the Menu icon  for the component and select Edit. You can then change the settings.</p>

Add risk correlation score

You must add conditional statements that assign a score to a targeted field.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select **ACE Properties**, then click **Risk Correlation Scoring**.
- 2 Click **Add**, then fill in the requested information.
- 3 Click **OK**.

Table 3-54 Option definitions

Option	Definition
Table	View the existing risk correlation scores.
Add	Add a risk correlation score.
Edit	Change the settings of the selected score.
Remove	Delete the selected score.
Enabled	Select to enable risk correlation scoring for the selected conditional statement. The setting is reflected in the Enabled column of the table.
Write	Write the new settings to the device.

Table 3-55 Option definitions

Option	Definition
Scoring Enabled	Select if you want to enable the conditional statement.
Type of Data	Select the type of data you want visible to the conditional statement. You can select either Event or Flow, or both.
Score Field	Search for the field to receive the desired score.
Lookup Field	Search for the field to match the source type against.
Source Type	Select the type of source to use for the comparison. If the selected source type contains a score value in addition to the matching value, then that score will be applied or a manually entered score can be given by selecting the checkbox in the Use Score column.
Value	Type or select the comparing value. The options available in this column vary based on the type of source selected in the previous column.
Use Score	Select the checkbox to use a manually entered score.
Score	The score to be given to the Score Field selected. A blended score can be applied to the score field when entering multiple rules in the grid.
Weight	Weight given to that row or source type for a blended score of the conditional statement. It cannot exceed 100%.
Add Row button	Click to add a new conditional row to the overall conditional statement.
Total Weight	Total of each of the rows or source types under the weight column.
Current Risk Score Range for	The range of the score that can be given to the field selected as the score field depending on the outcome of the conditional rows.

Using historical correlation

The historical correlation option allows you to correlate past events.

When a new vulnerability is discovered, it's important to check your historical events and logs to see if you were exploited in the past. Using ACE's easy network replay feature, historical events can be played through the **Risk Correlation** rule-less correlation engine and through the standard rule-based event correlation engine, letting you examine historical events against today's threat landscape. This can be useful in these situations:

- You did not have correlation set up at the time certain events were triggered and you notice that correlating them might have revealed valuable information.
- You are setting up a new correlation based on events triggered in the past and you want to test the new correlation to confirm that it provides the desired results.

Be aware of the following when using historical correlation:

- Real-time correlation is discontinued until you disable historical correlation.
- The risk distribution is skewed by event aggregation.
- When you move the risk manager back to real-time risk correlation, the thresholds must be tuned.

To set up and run historical correlation you must:

- 1 Add a historical correlation filter.
- 2 Run a historical correlation.
- 3 Download and view the correlated historical events.

See also

[Add and run historical correlation on page 116](#)

[Download and view the historical correlation events on page 117](#)

Add and run historical correlation

To correlate past events, you must set up a historical correlation filter, then run the correlation.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **ACE Properties**, then click **Historical**.
- 2 Click **Add**, fill in the information requested, then click **OK**.
- 3 Select **Enable Historical Correlation**, then click **Apply**.

Real-time correlation is discontinued until you disable historical correlation.

- 4 Select the filters you want to run, then click **Run Now**.

The ESM reviews the events, applies the filters, and packages the events that apply.

Table 3-56 Option definitions


Option	Definition
Enable historical correlation	Select if you want historical correlation enabled on the ACE. <div>  Real-time correlation is discontinued when historical correlation is enabled. </div>
Table	View the filters currently on the ACE.

Table 3-56 Option definitions *(continued)*

Option	Definition
Add	Add a filter to retrieve historical correlation event data.
Edit	Change the filter settings of the selected filter.
Remove	Delete a filter.
Run Now	Run the selected filters now. ESM reviews the events, applies the filters, and packages the events that apply.

Table 3-57 Option definitions

Option	Definition
Name	Type a name for this filter.
Time Frame	Select the timeframe to correlate the historical events.
Remaining fields	Select or type what you want to filter by. A hint for each field that you click appears at the bottom of the page.

See also

[Using historical correlation on page 116](#)

Download and view the historical correlation events

Once you have run the historical correlation, you can download and view the events it generated.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ACE Properties**, then click **Events and Logs | Get Events**.

The events that resulted from running the historical correlation are downloaded to the ESM.

- 2 Close **ACE Properties**.

- 3 To view the data:

- a On the system navigation tree, select the ACE device you just ran the historical data for.
- b On the time period drop-down list on the view toolbar, select the period of time you specified when setting up the run.

The view pane displays the results of the query.

See also

[Using historical correlation on page 116](#)

Application Data Monitor (ADM) settings

McAfee Application Data Monitor (ADM) tracks all use of sensitive data on the network, analyzing underlying protocols, session integrity, and application contents.

When ADM detects a violation, it preserves all details of that application session for use in incident response and forensics or for compliance audit requirements. At the same time, ADM provides visibility into threats that masquerade as legitimate applications.

ADM can detect when sensitive information is transmitted inside email attachments, instant messages, file transfers, HTTP posts, or other applications. Customize ADM's detection capabilities by defining your own dictionaries of sensitive and confidential information. ADM can then detect these sensitive data types, alert appropriate personnel, and log the transgression to maintain an audit trail.

ADM monitors, decodes, and detects anomalies in the following application protocols:

- File transfer: FTP, HTTP, SSL (setup and certificates only)
- Email: SMTP, POP3, NNTP, MAPI
- Chat: MSN, AIM/Oscar, Yahoo, Jabber, IRC
- Webmail: Hotmail, Hotmail DeltaSync, Yahoo mail, AOL Mail, Gmail
- P2P: Gnutella, bitTorrent
- Shell: SSH (detection only), Telnet

ADM accepts rule expressions and tests them against monitored traffic, inserting records into the event table of the database for each triggered rule. It stores the packet that triggered the rule in the event table's packet field. It also adds application level metadata to the dbsession and query tables of the database for every triggered rule. It stores a text representation of the protocol stack in the query table's packet field.

ADM can generate the following types of event:

- **Metadata** - ADM generates one metadata event for each network transaction, with details such as addresses, protocol, file type, file name. The application places the metadata events in the query table and groups the events through the session table. For example, if one FTP session transfers three files, ADM groups them together.
- **Protocol anomaly** - Protocol anomalies are hard-coded into the protocol modules and include events, such as a Transmission Control Protocol (TCP) packet being too short to contain a valid header and a Simple Mail Transfer Protocol (SMTP) server returning an invalid response code. Protocol anomaly events are rare and are placed in the event table.
- **Rule trigger** - Rule expressions generate rule trigger events, detecting anomalies in the metadata generated by the Internet Communications Engine (ICE). These events might include anomalies such as protocols used outside of normal hours or an SMTP server unexpectedly talking FTP. Rule trigger events must be rare and are placed in the event table.

The event table contains one record for each detected protocol anomaly or rule trigger event. The event records link to the session and query tables through the sessionid, where more detail about the network transfers (metadata events) that triggered the event is available. Each event also links to the packet table where the raw packet data for the packet that triggered the event is available.

The session table contains one record for each group of related network transfers (such as, a group of FTP file transfers on the same session). The session records link to the query table through the sessionid where more details about the individual network transfers (metadata events) are found. In addition, if a transfer within the session causes a protocol anomaly or triggers a rule, there is a link to the event table.

The query table contains one record for each metadata event (content transfers that take place on the network). The query records link to the session table with the sessionid. If the network transfer represented by the record triggers a protocol anomaly or rule, there is a link to the event table. There is also a link to the packet table using the text field where a textual representation of the full protocol or content stack is found.

Set ADM time zone

The ADM device is set to GMT but ADM code is expecting the device to be set to your time zone. As a result, rules use the time trigger as if you are in GMT and not when you expect them to.

You can set the ADM to the time zone that you expect. This is then taken into account when evaluating the rules.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ADM Properties**, then click **ADM Configuration**.
- 2 Click **Time Zone**, then select your time zone.
- 3 Click **OK**.

Display password on Session Viewer

The **Session Viewer** allows you to see the details of the latest 25,000 ADM queries in a session. The rules for some of the events might be password-related. You can select whether you want the passwords to display on the **Session Viewer**. By default, passwords aren't displayed.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **ADM Properties**, then click **ADM Configuration**.

The **Passwords** option states that logging is **Off**.

- 2 Click **Passwords**, select **Enable password logging**, then click **OK**.

The system executes the command and informs you when it's completed.

The **Passwords** option now states that logging is **On**.

Application Data Monitor (ADM) dictionaries

When writing ADM rules, use dictionaries that translate keys captured from the network into a defined value. Or, list keys without a value that defaults to Boolean true when the keys are present.

ADM dictionaries allow you to specify a file's keys quickly instead of having to write an individual rule for each word. For example, set up a rule to select email containing specific words, compile a dictionary with naughty words, and import that dictionary. You can create a rule like the following to check for emails with content that includes a word in the dictionary:

```
protocol == email && naughtyWords[objcontent]
```

When writing rules with the ADM rule editor, you can select the dictionary you want the rule to reference.



Dictionaries support up to millions of entries.

Adding a dictionary to a rule involves the following steps:

- 1 Setting up and saving a dictionary that lists the keys and, when needed, the values.
- 2 Managing the dictionary on the ESM.
- 3 Assigning the dictionary to a rule.

See also

[Setting up an ADM dictionary on page 120](#)

[Manage ADM dictionaries on page 123](#)

[Reference an ADM dictionary on page 121](#)

[ADM dictionary examples on page 122](#)

Setting up an ADM dictionary

A dictionary is a plain text file that consists of one entry per line. There are single column and double column dictionaries. Double columns include a key and a value.

Keys can be IPv4, MAC, number, regular expression, and string. Value types are boolean, IPv4, IPv6, MAC, number, and string. A value is optional and will default to boolean true if not present.

Values in a single or double column dictionary must be one of the supported ADM types: String, Regular Expression, Number, IPv4, IPv6, or MAC. ADM dictionaries must follow these formatting guidelines:

Type	Syntax Rules	Examples	Content Matched
String	<ul style="list-style-type: none"> Strings must be enclosed in double quotes Double quotes found within a String must be escaped using the backslash character before each quotation mark 	<p>"Bad Content"</p> <p>"He said, \"Bad Content\""</p>	<p>Bad Content</p> <p>He said, "Bad Content"</p>
Regular Expression	<ul style="list-style-type: none"> Regular expressions are enclosed with single forward slashes Forward slashes and reserved regular expression characters within the regular expression must be escaped with the backslash character 	<p>/[Aa]pple/</p> <p>/apple/i</p> <p>/ [0-9]{1,3}\.[0-9]{1,3}\.[0-9]\.[0-9]/</p> <p>/1\2 of all/</p>	<p>Apple or apple</p> <p>Apple or apple</p> <p>IP Addresses:</p> <p>1.1.1.1</p> <p>127.0.0.1</p> <p>1/2 of all</p>
Numbers	<ul style="list-style-type: none"> Decimal Values (0-9) Hexadecimal Values (0x0-9a-f) Octal Values (0-7) 	<p>Decimal Value</p> <p>Hexadecimal Value</p> <p>Octal Value</p>	<p>123</p> <p>0x12ab</p> <p>0127</p>

Type	Syntax Rules	Examples	Content Matched
Booleans	<ul style="list-style-type: none">• Can be true or false• All lower case	Boolean Literals	true false
IPv4	<ul style="list-style-type: none">• Can be written in standard dotted-quad notation• Can be written in CIDR notation• Can be written in long format with full masks	192.168.1.1 192.168.1.0/24 192.168.1.0/255.255.255.0	192.168.1.1 192.168.1.[0 – 255] 192.168.1.[0 – 255]

The following is true about dictionaries:

- Lists (multiple values separated by commas enclosed in brackets) are not allowed in dictionaries.
- A column can only consist of a single supported ADM type. This means that different types (string, regex, IPv4) cannot be mixed and matched within a single ADM dictionary file.
- They can contain comments. All lines starting with the pound character (#) are considered a comment within an ADM dictionary.
- Names can only consist of alphanumeric characters and underscores, and be of a total length less than or equal to 20 characters.
- Lists are not supported within them.
- Prior to ADM 8.5.0, they must be edited or created outside of the ESM with a text editor of your choice. They can be imported or exported from the ESM to facilitate modifying or creating new ADM dictionaries.

See also

[Application Data Monitor \(ADM\) dictionaries on page 119](#)

[Manage ADM dictionaries on page 123](#)

[Reference an ADM dictionary on page 121](#)

[ADM dictionary examples on page 122](#)

Reference an ADM dictionary


When a dictionary is imported to the ESM, you can refer to it when writing rules.

Before you begin

Import the dictionary to the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, click **New | ADM Rule**.
- 2 Add the requested information and drag-and-drop a logical element to the **Expression Logic** area.
- 3 Drag-and-drop the **Expression Component** icon  on the logical element.
- 4 On the **Expression Component** page, select the dictionary in the **Dictionary** field.
- 5 Fill in the remaining fields, then click **OK**.

See also[Application Data Monitor \(ADM\) dictionaries on page 119](#)[Setting up an ADM dictionary on page 120](#)[Manage ADM dictionaries on page 123](#)[ADM dictionary examples on page 122](#)**ADM dictionary examples**

The ADM engine can match object content or any other metric or property with a single column dictionary for true or false (exists in the dictionary or does not exist in the dictionary).

Table 3-58 Single column dictionary examples

Type of dictionary	Example
String dictionary with common spam words	"Cialis" "cialis" "Viagra" "viagra" "adult web" "Adult web" "act now! don't hesitate!"
Regular expression dictionary for authorization key words	/(password passwd pwd)[^a-z0-9]{1,3}(admin login password user)/i /(customer client)[^a-z0-9]{1,3}account[^a-z0-9]{1,3}number/i /fund[^a-z0-9]{1,3}transaction/i /fund[^a-z0-9]{1,3}transfer[^a-z0-9]{1,3}[0-9,.]+/i
String dictionary containing hash values for known bad executables	"fec72ceae15b6f60cbf269f99b9888e9" "fed472c13c1db095c4cb0fc54ed28485" "feddedb607468465f9428a59eb5ee22a" "ff3cb87742f9b56dfdb9a49b31c1743c" "ff45e471aa68c9e2b6d62a82bbb6a82a" "ff669082faf0b5b976cec8027833791c" "ff7025e261bd09250346bc9efdfc6c7c"
IP addresses of critical assets	192.168.1.12 192.168.2.0/24 192.168.3.0/255.255.255.0 192.168.4.32/27 192.168.5.144/255.255.255.240

Table 3-59 Double column dictionary examples

Type of dictionary	Example
String dictionary with common spam words and categories	"Cialis" "pharmaceutical" "cialis" "pharmaceutical" "Viagra" "pharmaceutical" "viagra" "pharmaceutical" "adult web" "adult" "Adult web" "adult" "act now! don't hesitate!" "scam"
Regular expression dictionary for authorization key words and categories	/(password passwd pwd)[^a-z0-9]{1,3}(admin login password user)/i "credentials" /(customer client)[^a-z0-9]{1,3}account[^a-z0-9]{1,3}number/i "pii" /fund[^a-z0-9]{1,3}transaction/i "sox" /fund[^a-z0-9]{1,3}transfer[^a-z0-9]{1,3}[0-9,.]+/i "sox"
String dictionary containing hash values for known bad executables and categories	"fec72ceae15b6f60cbf269f99b9888e9" "Trojan" "fed472c13c1db095c4cb0fc54ed28485" "Malware" "feddedb607468465f9428a59eb5ee22a" "Virus" "ff3cb87742f9b56dfdb9a49b31c1743c" "Malware" "ff45e471aa68c9e2b6d62a82bbb6a82a" "Adware" "ff669082faf0b5b976cec8027833791c" "Trojan" "ff7025e261bd09250346bc9efdfc6c7c" "Virus"
IP addresses of critical assets & groups	192.168.1.12 "Critical Assets" 192.168.2.0/24 "LAN" 192.168.3.0/255.255.255.0 "LAN" 192.168.4.32/27 "DMZ" 192.168.5.144/255.255.255.240 "Critical Assets"

See also

[Application Data Monitor \(ADM\) dictionaries](#) on page 119

[Setting up an ADM dictionary](#) on page 120

[Manage ADM dictionaries](#) on page 123

[Reference an ADM dictionary](#) on page 121

Manage ADM dictionaries

Once you set up and save a new dictionary, you must import it to the ESM. You can also export, edit, and delete it.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the **Policy Editor**, click **Tools**, then select **ADM Dictionary Manager**.

The **Manage ADM Dictionaries** screen lists the four default dictionaries (botnet, foullanguage, icd9_desc, and spamlist) and any dictionaries that were imported to the system.

- 2 Perform any of the available actions, then click **Close**.

Table 3-60 Option definitions



Option	Definition
Import	Click to import an ADM dictionary to the ESM.
Export	Click to export the selected ADM dictionary to a local file.
Edit	Click to edit the selected dictionary.
Delete	Delete the selected dictionary.
 When you delete a dictionary, any attempt to roll out a rule set that contains rules that reference this dictionary will fail to compile. If this dictionary is assigned to a rule, either rewrite the rule so it does not refer to the dictionary (see <i>Reference a dictionary</i>), or do not proceed with the deletion.	

Table 3-61 Option definitions

Option	Definition
Search	If you want to search for a specific entry, type it in the field and click.
Table	View the existing entries. You can add new entries and change or delete existing ones.

Table 3-62 Option definitions

Option	Definition
Dictionary	Browse to the dictionary file and upload it.
Key Type	Select the key type used in the dictionary.
 If there is a discrepancy between what you selected in the Key Type and Value Type fields and what the file contains, you are informed that the data is invalid.	
Value Type	Select the type of value used in the dictionary.

See also

[Application Data Monitor \(ADM\) dictionaries on page 119](#)

[Setting up an ADM dictionary on page 120](#)

[Reference an ADM dictionary on page 121](#)

[ADM dictionary examples on page 122](#)

ADM rule reference material

This appendix includes material that can assist you when adding ADM rules to the **Policy Editor**.

See also

[ADM rules syntax on page 124](#)

[ADM rule term types on page 127](#)

[ADM rule metric references on page 129](#)

[Protocol-specific properties on page 131](#)

ADM rules syntax

The ADM rules are very similar to C expressions.

The main difference is a more extensive set of literals (numbers, strings, regular expressions, IP addresses, MAC addresses, and Booleans). String terms can be compared with string and Regex literals to test their content but they can also be compared with numbers to test their length. Numeric, IP address, and MAC address terms can

only be compared with the same type of literal value. The only exception is that everything can be treated as a Boolean to test for its existence. Some terms can have multiple values, for example the following rule would trigger for PDF files inside .zip files: `type == application/zip && type == application/pdf`.

Table 3-63 Operators

Operator	Description	Example
&&	Logical AND	<code>protocol == http && type == image/gif</code>
	Logical OR	<code>time.hour < 8 time.hour > 18</code>
^^	Logical XOR	<code>email.from == "a@b.com" ^^ email.to == "a@b.com"</code>
!	Unary NOT	<code>!(protocol == http protocol == ftp)</code>
==	Equal	<code>type == application/pdf</code>
!=	Not equal	<code>srcip != 192.168.0.0/16</code>
>	Greater	<code>objectsize > 100M</code>
>=	Greater or equal	<code>time.weekday >= 1</code>
<	Less	<code>objectsize < 10K</code>
<=	Less or equal	<code>time.hour <= 6</code>

Table 3-64 Literals

Literal	Example
Number	1234, 0x1234, 0777, 16K, 10M, 2G
String	"a string"
Regex	/[A-Z] [a-z]+/
IPv4	1.2.3.4, 192.168.0.0/16, 192.168.1.0/255.255.255.0
MAC	aa:bb:cc:dd:ee:ff
Bool	true, false


Table 3-65 Type operator compatibility

Type	Operators	Notes
Number	<code>==, !=, >, >=, <, <=</code>	
String	<code>==, !=</code>	Compare content of string with String/Regex
String	<code>>, >=, <, <=</code>	Compare length of string
IPv4	<code>==, !=</code>	
MAC	<code>==, !=</code>	
Bool	<code>==, !=</code>	Compare against true/false, also supports implied comparison with true, for example the following tests whether the email.bcc term occurs: <code>email.bcc</code>

Table 3-66 ADM regex grammar

Basic operators	
	Alternation (or)
*	Zero or more

Table 3-66 ADM regex grammar *(continued)*

Basic operators	
+	One or more
?	Zero or one
()	Grouping (a b)
{ }	Repeating Range {x} or {,x} or {x,} or {x,y}
[]	Range [0-9a-z] [abc]
[^]	Exclusive Range [^abc] [^0-9]
.	Any Character
\	Escape Character
Escapes	
\d	Digit [0-9]
\D	Non-Digit [^0-9]
\e	Escape (0x1B)
\f	Form Feed (0x0C)
\n	Line Feed (0x0A)
\r	Carriage Return (0x0D)
\s	White Space
\S	Not White Space
\t	Tab (0x09)
\v	Vertical Tab (0x0B)
\w	Word [A-Za-z0-9_]
\W	Not Word
\x00	Hex Representation
\0000	Octal Representation
^	Start of line
\$	End of line
 The start of line and end of line anchors (^ and \$) don't work for objcontent.	
POSIX character classes	
[[:alnum:]]	Digits and letters
[[:alpha:]]	All letters
[[:ascii:]]	ASCII Characters

POSIX character classes	
[[:blank:]]	Space and tab
[[:cntrl:]]	Control characters
[[:digit:]]	Digits
[[:graph:]]	Visible characters
[[:lower:]]	Lowercase letters
[[:print:]]	Visible characters and spaces
[[:punct:]]	Punctuation and Symbols
[[:space:]]	All whitespace characters
[[:upper:]]	Uppercase characters
[[:word:]]	Word characters
[[:xdigit:]]	Hexadecimal Digit

See also

[ADM rule reference material on page 124](#)

[ADM rule term types on page 127](#)

[ADM rule metric references on page 129](#)

[Protocol-specific properties on page 131](#)

[Protocol anomalies on page 132](#)


ADM rule term types

All terms in an ADM rule have a specific type.

Each term is either an IP address, a MAC address, a number, a string, or a boolean. In addition there are two extra literal types: regular expressions and lists. A term of a specific type can generally only be compared against a literal of the same type or a list of literals of the same type (or a list of lists of ...). There are three exceptions to this rule:

- 1 A string term can be compared against a numeric literal to test its length. The following rule triggers if a password is fewer than eight characters long (password is a string term): password < 8
- 2 A string term can be compared against a regular expression. The following rule triggers if a password only contains lower case letters: password == /^[a-z]+\$/
- 3 All terms can be tested against boolean literals to test whether they occur at all. The following rule triggers if an email has a CC address (email.cc is a string term): email.cc == true

Type	Format description
IP addresses	<ul style="list-style-type: none">• IP address literals are written in standard dotted-quad notation, they are not enclosed in quotes: 192.168.1.1• IP addresses can have a mask written in standard CIDR notation, there must not be any white space between the address and the mask: 192.168.1.0/24• IP addresses can also have masks written out in long form: 192.168.1.0/255.255.255.0
Mac addresses	<ul style="list-style-type: none">• MAC address literals are written using standard notation, as with IP addresses, they are not enclosed in quotes: aa:bb:cc:dd:ee:ff

Type	Format description
Numbers	<ul style="list-style-type: none"> • All numbers in ADM rules are 32-bit integers. They can be written in decimal: 1234 • They can be written in hexadecimal: 0xabcd • They can be written in octal: 0777 • They can have a multiplier appended to multiply by 1024 (K), 1048576 (M) or 1073741824 (G): 10M
Strings	<ul style="list-style-type: none"> • Strings are enclosed in double quotes: "this is a string" • Strings can use standard C escape sequences: "\tThis is a \"string\" containing\x20escape sequences\n" • When comparing a term against a string, the whole term must match the string. If an email message has a from address of someone@somewhere.com then the following rule will not trigger: email.from == "@somewhere.com" • To match only a part of a term, a regular expression literal should be used instead. String literals must be used when possible because they are more efficient. <div>  All email address and URL terms are normalized before matching so it is not necessary to take account of things like comments within email addresses. </div>
Booleans	<ul style="list-style-type: none"> • The boolean literals are true and false.

Type	Format description
Regular expressions	<ul style="list-style-type: none"> Regular expression literals use the same notation as languages like Javascript and Perl, enclosing the regular expression in forward slashes: <code>/[a-z]+/</code> Regular expressions can be followed by standard modifier flags, though "i" is the only one currently recognized (case-insensitive): <code>/[a-z]+/i</code> Regular expression literals should use the POSIX Extended syntax. Currently Perl extensions work for all terms except the content term but this might change in future versions. When comparing a term against a regular expression, the regular expression matches any substring within the term unless anchor operators are applied within the regular expression. The following rule triggers if an email is seen with an address of "someone@somewhere.com": <code>email.from == /@somewhere.com/</code>
Lists	<ul style="list-style-type: none"> List literals consist of one or more literals enclosed in square brackets and separated by commas: <code>[1, 2, 3, 4, 5]</code> Lists might contain any kind of literal, including other lists: <code>[192.168.1.1, [10.0.0.0/8, 172.16.128.0/24]]</code> Lists must only contain one kind of literal, it's not valid to mix strings and numbers, strings and regular expressions, IP addresses and MAC addresses. When a list is used with any relational operator other than not-equal (<code>!=</code>), then the expression is true if the term matches any literal in the list. The following rule triggers if the source IP address matches any of the IP addresses in the list: <code>srcip == [192.168.1.1, 192.168.1.2, 192.168.1.3]</code> It is equivalent to: <code>srcip == 192.168.1.1 srcip == 192.168.1.2 srcip == 192.168.1.3</code> When used with the not-equal (<code>!=</code>) operator, the expression is true if the term doesn't match all of the literals in the list. The following rule triggers if the source IP address is not 192.168.1.1 or 192.168.1.2: <code>srcip != [192.168.1.1, 192.168.1.2]</code> It is equivalent to: <code>srcip != 192.168.1.1 && srcip != 192.168.1.2</code> Lists might also be used with the other relational operators, though it doesn't make a lot of sense. The following rule triggers if the object size is greater than 100 or if the object size is greater than 200: <code>objectsize > [100, 200]</code> It is equivalent to: <code>objectsize > 100 objectsize > 200</code>

See also[ADM rule reference material on page 124](#)[ADM rules syntax on page 124](#)[ADM rule metric references on page 129](#)[Protocol-specific properties on page 131](#)[Protocol anomalies on page 132](#)**ADM rule metric references**

Here are lists of metric references for ADM rule expressions, which are available on the **Expression Component** page when you are adding an ADM rule.

For Common Properties and Common Anomalies, the parameter-type value you can enter for each one is shown in parentheses after the metric reference.

Common Properties

Property or term	Description
Protocol (Number)	The application protocol (HTTP, FTP, SMTP)
Object Content (String)	The content of an object (text inside a document, email message, chat message). Content matching is not available for binary data. Binary objects can, however, be detected using Object Type (objtype)

Property or term	Description
Object Type (Number)	Specifies the type of the content as determined by ADM (Office Documents, Messages, Videos, Audio, Images, Archives, Executables)
Object Size (Number)	Size of the object. Numeric multipliers K, M, G can be added after the number (10K, 10M, 10G)
Object Hash (String)	The hash of the content (currently MD5)
Object Source IP Address (Number)	The source IP address of the content. IP address can be specified as 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Object Destination IP Address (Number)	The destination IP address of the content. IP address can be specified as, 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Object Source Port (Number)	The source TCP/UDP port of the content
Object Destination Port (Number)	The destination TCP/UDP port of the content
Object Source IP v6 Address (Number)	The source IPv6 address of the content
Object Destination IPv6 Address (Number)	The destination IPv6 address of the content
Object Source MAC Address (mac name)	The source MAC address of the content (aa:bb:cc:dd:ee:ff)
Object Destination MAC Address (mac name)	The destination MAC address of the content (aa:bb:cc:dd:ee:ff)
Flow Source IP Address (IPv4)	Source IP address of the flow. IP address can be specified as 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Flow Destination IP Address (IPv4)	Destination IP address of the flow. IP address can be specified as 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Flow Source Port (Number)	Source TCP/UDP port of flow
Flow Destination Port (Number)	Destination TCP/UDP port of flow
Flow Source IPv6 Address (Number)	Source IPv6 address of the flow
Flow Destination IPv6 Address (Number)	Destination IPv6 address of the flow
Flow Source MAC Address (mac name)	Source MAC address of the flow
Flow Destination MAC Address (mac name)	Destination MAC address of flow
VLAN (Number)	Virtual LAN ID
Day of Week (Number)	The day of the week. Valid values are 1–7; 1 is Monday.
Hour of Day (Number)	The hour of the day set to GMT. Valid values are 0–23.
Declared Content Type (String)	Type of the content as specified by the server. In theory, Object Type (objtype) is always the actual type and Declared Content-type (content-type) is not trustworthy because it can be spoofed by the server/application.
Password (String)	Password used by the application for authentication.
URL (String)	Website URL. Applies only to HTTP protocol.
File Name (String)	Name of the file being transferred.
Display Name (String)	
Host Name (String)	Host name as specified in DNS lookup.

Common Anomalies

- User logged off (Boolean)
- Authorization error (Boolean)
- Authorization successful (Boolean)
- Authorization failed (Boolean)

See also

ADM rule reference material on page 124

ADM rules syntax on page 124

ADM rule term types on page 127

Protocol-specific properties on page 131

Protocol anomalies on page 132

Protocol-specific properties

In addition to providing properties that are common across most protocols, ADM also provides protocol-specific properties that can be used with ADM rules. All protocol-specific properties are also available in the **Expression Component** page when adding an ADM rule.

Examples of protocol-specific properties

These properties apply to these tables:

```
*   Detection only
**  No decryption, captures X.509 certificates and encrypted data
*** Via RFC822 module
```

Table 3-67 File transfer protocol modules

FTP	HTTP	SMB*	SSL**
Display Name	Display Name	Display Name	Display Name
File Name	File Name	File Name	File Name
Host Name	Host Name	Host Name	Host Name
URL	Referer		
	URL		
	All HTTP headers		

Table 3-68 Email protocol modules

DeltaSync	MAPI	NNTP	POP3	SMTP
Bcc***	Bcc	Bcc***	Bcc***	Bcc***
Cc***	Cc	Cc***	Cc***	Cc***
Display Name	Display Name	Display Name	Display Name	Display Name
From***	From	From***	From***	From***
Host Name	Host Name	Host Name	Host Name	Host Name
Subject***	Subject	Subject***	Subject***	To***
To***	To	To***	To***	Subject***
	User Name		User Name	

Table 3-69 Webmail protocol modules

AOL	Gmail	Hotmail	Yahoo
Attachment Name	Attachment Name	Attachment Name	Attachment Name
Bcc***	Bcc***	Bcc***	Bcc***
Cc***	Cc***	Cc***	Cc***
Display Name	Display Name	Display Name	Display Name
File Name	File Name	File Name	File Name
Host Name	Host Name	Host Name	Host Name
From***	From***	From***	From***
Subject***	Subject***	Subject***	Subject***
To***	To***	To***	To***

See also[ADM rule reference material on page 124](#)[ADM rules syntax on page 124](#)[ADM rule term types on page 127](#)[ADM rule metric references on page 129](#)[Protocol anomalies on page 132](#)**Protocol anomalies**

Beyond the common properties and protocol-specific properties, ADM also detects hundreds of anomalies in low-level, transport, and application protocols. All protocol anomaly properties are of type Boolean and are available in the **Expression Component** page when you are adding an ADM rule.

Table 3-70 IP

Term	Description
ip.too-small	IP packet is too small to contain a valid header.
ip.bad-offset	IP data offset goes past end of packet.
ip.fragmented	IP packet is fragmented.
ip.bad-checksum	IP packet checksum doesn't match data.
ip.bad-length	IP packet totlen field goes past end of packet.

Table 3-71 TCP

Term	Description
tcp.too-small	TCP packet is too small to contain a valid header.
tcp.bad-offset	TCP packet's data offset goes past end of packet.
tcp.unexpected-fin	TCP FIN flag set in non-established state.
tcp.unexpected-syn	TCP SYN flag set in established state.
tcp.duplicate-ack	TCP packet ACKs data that's already been ACKed.
tcp.segment-outsidewindow	TCP packet is outside the window (TCP module's small window, not real window).
tcp.urgent-nonzero-withouturg- flag	TCP urgent field is non-zero but URG flag isn't set.

Table 3-72 DNS

Term	Description
dns.too-small	DNS packet is too small to contain a valid header.
dns.question-name-past-end	DNS question name goes past the end of the packet.
dns.answer-name-past-end	DNS answer name goes past the end of the packet.
dns.ipv4-address-length-wrong	IPv4 address in DNS response is not 4 bytes long.
dns.answer-circular-reference	DNS answer contains circular reference.

See also[ADM rules syntax on page 124](#)[ADM rule term types on page 127](#)[ADM rule metric references on page 129](#)[Protocol-specific properties on page 131](#)

Database Event Monitor (DEM) settings

McAfee Database Event Monitor (DEM) consolidates database activity into a central audit repository and provides normalization, correlation, analysis, and reporting of that activity. If network or database server activity matches known patterns indicating malicious data access, DEM generates an alert. In addition, all transactions are logged for use in compliance.

DEM enables you to manage, edit, and adjust database monitoring rules from the same interface that provides analysis and reporting. You can easily adjust specific database monitoring profiles (which rules are enforced, what transactions are logged), reducing false-positives and improving security overall.

DEM non-intrusively audits the interactions of your users and applications with your databases by monitoring network packets similar to intrusion detection systems. To ensure that you can monitor all database server activity over the network, coordinate your initial DEM deployment with your networking, security, compliance, and database teams.

Your network teams use span ports on switches, network taps, or hubs to replicate database traffic. This process allows you to listen to or monitor the traffic on your database servers and create an audit log.

Visit the McAfee website for information about supported database server platforms and versions.

Operating system	Database	DEM appliance
Windows (all versions)	Microsoft SQL Server ¹	MSSQL 7, 2000, 2005, 2008, 2012
Windows, UNIX/Linux (all versions)	Oracle ²	Oracle 8.x, 9.x, 10 g, 11 g (c), 11 g R2 ³
	Sybase	11.x, 12.x, 15.x
	DB2	8.x, 9.x, 10.x
	Informix (available in 8.4.0 and later)	11.5
Windows, UNIX/Linux (all versions)	MySQL	Yes, 4.x, 5.x, 6.x
	PostgreSQL	7.4.x, 8.4.x, 9.0.x, 9.1.x
	Teradata	12.x, 13.x, 14.x
	InterSystems Cache	2011.1.x
UNIX/Linux (all versions)	Greenplum	8.2.15
	Vertica	5.1.1-0

Operating system	Database	DEM appliance
Mainframe	DB2/zOS	All versions
AS400	DB2	All versions
<ol style="list-style-type: none"> 1 Packet decryption support for Microsoft SQL Server is available in version 8.3.0 and later. 2 Packet decryption support for Oracle is available in version 8.4.0 and later. 3 Oracle 11 g is available in version 8.3.0 and later. 		

The following applies to these servers and versions:

- Both 32-bit and 64-bit versions of operating systems and database platforms are supported.
- MySQL is supported on Windows 32-bit platforms only.
- Packet decryption is supported for MSSQL and Oracle.

Update DEM license

The DEM comes with a default license. If you change the capabilities of the DEM, McAfee sends you a new license in an email message and you must update it.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.
- 2 Click **License | Update License**, then paste the information sent to you by McAfee in the field.
- 3 Click **OK**.

The system updates the license and informs you when it's done.

- 4 Roll out the policy to the DEM.

Table 3-73 Option definitions

Option	Definition
Update License	Click to update the DEM license.
Update License page	Copy the license sent to you by McAfee, then paste it here and click OK .

Sync DEM configuration files

When DEM configuration files are out of sync with the DEM device, you must write the configuration files to the DEM.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.
- 2 Click **Sync Files**.

A message displays the status of the sync.

Configure advanced DEM settings

These advanced settings change or increase the performance of the DEM.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.
- 2 Click **Advanced**, then define the settings or deselect options if you begin to experience a heavy load on the DEM.
- 3 Click **OK**.

Table 3-74 Option definitions



Option	Definition
Define these settings as needed.	
Log file detail level	Set the level of detail for the log information sent from the DEM agent to the DEM Manager. These are the three options: Information , Warn , and Debug . <div>  If you select Debug, the information is very detailed and can consume a great deal of disk space. </div>
Agent Registry Port and Agent Service Port	Change default agent registry and service ports. These are the ports that are used to communicate with the agent.
Use encryption	Select to encrypt or not encrypt the information sent to the DEM manager from the DEM agent. This log decrypts when it's received.
Kerberos server IP	Enter the Kerberos server IP address if you want to retrieve user names from Kerberos protocol analysis for database authentication using Windows Integrated Security. <div>  Multiple IP, Port, and VLAN settings may be specified using the following format: IP;PORT;VLAN;IP;PORT (for example, 10.0.0.1;88;11,10.0.0.2;88;12). IPv6 is also supported using this same format. </div>
Shared memory	Choose the size of the buffer that the DEM uses to process database events. Increasing the size of the buffer provides better performance.
Event repository	Select the location from which the events are retrieved. If you select File , the file on the local DEM will be read and those events are parsed. If you select EDB , events are collected from the database.

Table 3-75 Option definitions

Option	Definition
Deselect any of these options if you begin to experience a heavy load on the DEM.	
McAfee Firewall packet capture	Provides a faster way for the DEM to parse the database data.
Transaction tracking	Tracks database transactions and auto reconcile changes. Deselect to increase DEM speed.
User identity tracking	Tracks user's identities when they aren't being propagated to the database because generic user names are being used to access the database. Deselect to increase DEM speed.
Sensitive data masking	Prevents unauthorized viewing of sensitive data by replacing the sensitive information with a generic user-defined string, called the mask. Deselect to increase DEM speed.
Local host auditing	Audits local hosts to track unknown access paths into the database and send events in real time. Deselect to increase DEM speed.
Query parsing	Performs query inspections. Deselect to increase DEM speed.

Table 3-75 Option definitions *(continued)*

Option	Definition
First result row capture	Allows you to view the first result row of a query when you retrieve a packet for an event and a Select Statement's severity has been set to less than 95. Deselect to increase DEM speed.
Bind variable support	Reuses the Oracle bind variable over and over without incurring the overhead of re-parsing the command each time it's executed.

Apply DEM configuration settings

Changes made to DEM configuration settings must be applied to the DEM. Should you neglect to apply any configuration changes, the **Apply** option on **DEM Configuration** allows you to do so for all DEM configuration settings.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.
- 2 Click **Apply**.

A message informs you when the configuration settings are written to the DEM.

Defining actions for DEM events

Action Management settings on the DEM define actions and operations for events, which are used in the DEM's filtering rules and data access policies. You can add custom actions and set the **Operation** for default and custom actions.

The DEM comes with default actions, which you can see by clicking **Edit Global** on the **Action Management** page, and these default operations:

- none
- ignore
- discard
- scripts
- reset

If you select **Script** as the operation, an alias name (SCRIPT ALIAS) is required, pointing to the actual script (SCRIPT NAME) that must be executed when the criticality event occurs. The script is passed two environment variables, ALERT_EVENT and ALERT_REASON. ALERT_EVENT contains a colon-separated list of metrics. DEM provides a sample bash script /home/auditprobe/conf/sample/process_alerts.bash to demonstrate how the criticality action can be captured in a script.

When working with actions and operations, keep this in mind:

- Actions are listed in order of priority.
- An event does not take an action such as sending an SNMP trap or page unless you specify this as the alert action.
- When a rule qualifies for more than one alert level, only the highest alert level is actionable.
- Events are written to an event file regardless of the action. The only exception is a **Discard** operation.

See also

[Add a DEM action on page 137](#)

[Edit a DEM custom action on page 137](#)

[Set the operation for a DEM action on page 138](#)

Add a DEM action

If you add an action to DEM action management, it appears on the list of available actions for a DEM rule in the **Policy Editor**. You can then select it as the action for a rule.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, click the **Policy Editor** icon , then click **Tools | DEM Action Manager**.

The **DEM Action Management** page lists the existing actions in order of priority.



You can't change the priority order of the default actions.

- 2 Click **Add**, then enter a name and description for this action.

You can't delete a custom action once it's added.

- 3 Click **OK**.

The new action is added to the **DEM Action Management** list.

The default operation for a custom action is **None**. To change this, see *Set the operation for a DEM action*.

Table 3-76 Option definitions

Option	Definition
Action Name	Type the name for this action.
Description	(Optional) Type a description of this action.

See also

[Defining actions for DEM events on page 136](#)

[Edit a DEM custom action on page 137](#)

[Set the operation for a DEM action on page 138](#)

Edit a DEM custom action

Once you have added an action to the DEM action management list, you might need to edit its name or change its priority.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, click the **Policy Editor** icon , then click **Tools | DEM Action Manager**.

- 2 Click the custom action you need to change and do one of the following:
 - To change the priority order, click the up or down arrows until it is in the correct position.
 - To change the name or description, click **Edit**.

- 3 Click **OK** to save your settings.

See also

[Defining actions for DEM events on page 136](#)

[Add a DEM action on page 137](#)

[Set the operation for a DEM action on page 138](#)

Set the operation for a DEM action

All rule actions have a default operation. When you add a custom DEM action, the default operation is **None**. You can change the operation of any action to **Ignore**, **Discard**, **Script**, or **Reset**.

Task



For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **DEM Properties**, then click **Action Management**.
- 2 Highlight the action you want to edit, then click **Edit**.
- 3 Select an operation, then click **OK**.

Table 3-77 Option definitions

Option	Definition
Operation	Select what you want this action to do if the rule triggers an event. The options are: <ul style="list-style-type: none"> • None — Doesn't do anything. • Ignore — Keeps the event in the database, but it doesn't show up in the user interface. • Discard — Doesn't keep the event in the database or show in the user interface. • Script — Executes a script that you define. • Reset — Attempts to break the database connection by sending TCP RST packets to the client and server.
Script Name	If you selected Script as the operation, set the script name. If there aren't any scripts on the drop-down list, click Script Name and select a script file on the Script File Management page.

Table 3-78 Option definitions

Option	Definition
Add	Click to add a new action. <div>  You can't delete a custom action once it has been added. </div>
Edit	Change the name or description of the selected custom action.
Move up and Move Down arrows	Change the order of the custom actions. <div>  You can't change the priority order of the default actions </div>

See also

[Defining actions for DEM events on page 136](#)

[Add a DEM action on page 137](#)

[Edit a DEM custom action on page 137](#)

Working with sensitive data masks

Sensitive data masks prevent unauthorized viewing of sensitive data by replacing the sensitive information with a generic string, called the mask. Three standard sensitive data masks are added to the ESM database when you add a DEM device to the system, but you can add new ones and edit or remove existing ones.

These are the standard masks:

- Sensitive mask name: Credit Card Number Mask

Expression: ((4\d{3})|(5[1-5]\d{2})|(6011))-?\d{4}-?\d{4}|3[4,7]\d{13}

Substring Index: \0

Masking Pattern: #####-####-####-####

- Sensitive mask name: Mask First 5 Chars of SSN

Expression: (\d\d\d\d-\d\d)-\d\d\d\d\d

Substring Index: \1

Masking Pattern: ###-##

- Sensitive mask name: Mask User Password in SQL Stmt

Expression: create\s+user\s+(\w+)\s+identified\s+by\s+(\w+)

Substring Index: \2

Masking Pattern: *****

See also

[Manage sensitive data masks on page 139](#)

Manage sensitive data masks


To protect sensitive information entered on the system, you can add sensitive data masks and edit or remove existing ones.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **DEM Properties**, then click **Sensitive Data Masks**.
- 2 Select an option, then enter the requested information.
- 3 Click **OK**, then click **Write** to add the settings to the DEM.

Table 3-79 Option definitions

Option	Definition
Sensitive mask name	Type a name for the sensitive data mask.
Expression	Type a REGEX expression conforming to Perl-Compatible Regular Expression (PCRE) syntax (see <i>Work with sensitive data masks</i> for examples).
Sub String Index	Select an option. <div> Options are added based on the number of braces () used in the expression. If you have one set of braces, your options are \0 and \1. If you select \0, the whole string is replaced with the mask. If you select \1, only the strings are replaced by the mask.</div>
Masking Pattern	Type the masking pattern that must appear in place of the original value.

See also

[Working with sensitive data masks on page 139](#)

Managing user identification

Much of security is based on a simple principle that users have to be identified and distinguished from each other, yet generic user names are often used to access the database. Identifier management provides a way to capture the real user name if it exists anywhere in the query, using REGEX patterns.

Applications can be quite easily instrumented to take advantage of this security feature. Two defined identifier rules are added to the ESM database when you add a DEM device to the system.

- Identifier Rule Name: Get User Name from SQL Stmt

Expression: `select\s+username=(\w+)`

Application: Oracle

Substring Index: \1

- Identifier Rule Name: Get User Name from Stored Procedure

Expression: `sessionStart\s+@appname='(\w+)', @username='(\w+)'`,

Application: MSSQL

Substring Index: \2



Advanced user correlation is possible by correlating the DEM, application, web server, system, and identity and access management logs in the ESM.

See also

[Add a user identifier rule on page 140](#)

Add a user identifier rule



To associate database queries with individuals, you can use the existing user identifier rules or add a rule.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **DEM Properties**, then click **Identifier Management**.
- 2 Click **Add**, then enter the information requested.
- 3 Click **OK**, then click **Write** to write the settings to the DEM.

Table 3-80 Option definitions

Option	Definition
Identifier rule name	Type a name for this identifier rule.
Expression	Type a REGEX expression conforming to PCRE syntax (see <i>Manage user identification</i> for examples).  The REGEX operator implements the PCRE library for pattern matching using the same semantics as Perl 5. The general syntax is: <"metric name"> REGEX <"pattern">. For information on PCRE, see http://www.pcre.org .
Application	Select the application (database type) where the information is observed.
Sub String Index	Select a sub string.  Options are added based on the number of braces () used in the expression. If you have one set of braces, your options are: \0 and \1.

See also

Managing user identification on page 140

About database servers

Database servers monitor database activity. If activity seen on a database server matches a known pattern that indicates malicious data access, an alert is generated. Each DEM can monitor a maximum of 255 database servers.

DEM currently supports the following database servers and versions.

OS	Database	DEM Appliance
Windows (all versions)	Microsoft SQL Server ¹	MSSQL 7, 2000, 2005, 2008, 2012
Windows UNIX/Linux (all versions)	Oracle ²	Oracle 8.x, 9.x, 10g, 11g ³ , 11g R2
	Sybase	11.x, 12.x, 15.x
	DB2	8.x, 9.x, 10.x
	Informix (see note 4)	11.5
	MySQL	Yes, 4.x, 5.x, 6.x
	PostgreSQL	7.4.x, 8.4.x, 9.0.x, 9.1.x
	Teradata	12.x, 13.x, 14.x
	InterSystem Cache	2011.1.x
	Greenplum	8.2.15
UNIX/Linux (all version)	Vertica	5.1.1-0
Mainframe	DB2/zOS	All versions

OS	Database	DEM Appliance
AS 400	DB2	All versions
<ol style="list-style-type: none"> 1 Packet decryption support for Microsoft SQL Server is available in versions 8.3.0 and later. 2 Packet decryption support for Oracle is available in versions 8.4.0 and later. 3 Oracle 11g is available in version 8.3.0 and later. 4 Informix support is available in versions 8.4.0 and later. 		



- Both 32-bit and 64-bit versions of OS and database platforms are supported.
- MySQL is supported on Windows 32-bit platforms only.
- Packet decryption is supported for MSSQL & Oracle.

See also

[Manage database servers on page 142](#)

[Manage database discovery notifications on page 144](#)

Manage database servers

The **Database Server** page is the starting point for managing settings for all database servers for your DEM device.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **DEM Properties**, then click **Database Servers**.
- 2 Select any of the available options.
- 3 Click **OK**.

Table 3-81 Option definitions

Option	Definition
Table	View the list of database servers on the DEM.
Add	Add a new database server.
Add Agent	The McAfee DEM agent is no longer sold. If you purchased the DEM agent license in a version prior to 9.2 and need assistance, please call McAfee Support.
Edit	Make changes to the selected database server.
Remove	Delete the selected database server.
Copy	Create a copy of the selected database server.
Write	Apply the settings for the database servers to the DEM.
Enable	Click if you want to receive an alert notification when new database servers are found.
Disable	Click if you want to disable notification.

Table 3-82 Option definitions

Option	Definition
Enabled	Select if you want the DEM to process data for this database server. If disabled, the configuration settings are saved on the ESM for later use.
Storage Pool	Click and select a storage pool if you want the data received sent to the ELM device.

Table 3-82 Option definitions (continued)





Option	Definition
Zone	If you have zones defined on your system, select the zone you want this database server assigned to. To add a zone to the system, click Zone .
Database Type	<p>Select the type of database. The remaining fields vary, based on what you select in this field.</p> <p> The DEM implements PI JDBC Driver to connect to the PI System. PI SQL Data Access Server (DAS) serves as a gateway between PI JDBC Driver and PI OLEDB. It provides secure network communication (https) to PI JDBC and executes queries as a PI OLEDB consumer (client).</p>
Database Server Name	<p>Type a name for this database server.</p> <p> If you selected PIServer in the Database Type field, this field is DAS Datasource Name, which is the name of the PI Server being accessed by the Data Access Server (DAS) gateway. It must be exactly as specified in the DAS configuration. It can be the same as the DAS hostname if the DAS server is installed on the same host as the PI Server.</p>
Device URL	If you have one available, type the URL address where you can view database server information. If the URL address you entered includes the address of a third-party application, append variables to the URL address by clicking the variables icon  .
IP Address	Enter a single IP address for this database server or DAS in the IP address field. This field accepts a single IP address in IPv4 dot notation. Masks are not acceptable for these IP addresses.
Priority Group	Assign the database server to a priority group. This allows you to balance the load of data processed by the DEM. You can view a list of the database servers and the priority groups they belong to on the Database Servers table.
Virtual LAN ID	Type the virtual LAN ID, if required. If you enter the value "0," it represents all VLANs.
Encoding Option	Select one of the available options: None, UTF8, and BIG5.
Select Special Options	<p>Select one of the following (options available depend on database type selected):</p> <ul style="list-style-type: none"> • Port Redirection must be specified when you are monitoring an Oracle server running on a Windows platform. • Server Uses Named Pipes must be selected if the database server uses the Named Pipes SMB protocol. The default pipe name for MSSQL is \\.\pipe\sql\query and the default port is 445. • Dynamic Ports must be selected if the database server has TCP Dynamic Ports enabled. Enter a port number for the database server or DAS in the Port field. The port is the service port of the database server where it is listening for connections. Common default port numbers are: 1433 for Microsoft SQL Server (MSSQL), 1521 for Oracle, 3306 for MySQL, 5461 for Data Access Server (DAS), and 50000 for DB2/UDB.
Kerberos authentication	Select if you want the SQL server to perform Kerberos authentication.
RSA encryption type	Select either None or RSA .
RSA encryption level	Select the appropriate option based on your choice for Forced Encryption: Decrypt Login Packets if Forced Encryption is No; Decrypt All Packets if Forced Encryption is Yes.
RSA Key	<p>Click Browse and select the RSA Key file, or copy the key from the file and paste it in the RSA Key field.</p> <p> The ESM console accepts only RSA certificates of .pem file format with no password.</p>

Table 3-82 Option definitions *(continued)*

Option	Definition
Username	Type the user name for PI DAS login. Because PI DAS is installed on Windows, it uses Windows integrated security. The user name must be specified as domain\login.
Password	Type the password for the DAS user name.
Retrieve archive logs	Select if you want the PI Server Archives database polled for changes to ALL Point.
Points to monitor	Enter a list of comma-separated points so only those points are monitored.

See also

[About database servers](#) on page 141


[Manage database discovery notifications](#) on page 144

Manage database discovery notifications

The DEM has a database discovery feature that provides an exception list of database servers that are not being monitored. This allows a security administrator to discover new database servers added to the environment and illegal listener ports opened to access data from databases. When this is enabled, you receive an alert notification that shows up on the **Event Analysis** view. You can then choose whether to add the server to those being monitored on your system.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **DEM Properties**, then click **Database Servers** | **Enable**.
You are notified when it's enabled.
- 2 Click **OK** to close **DEM Properties**.
- 3 To view the notifications, click the DEM device on the system navigation tree, then select **Event Views** | **Event Analysis**.
- 4 To add the server to your system, select the **Event Analysis** view, then click the **Menu** icon  and select **Add Server**.

See also

[About database servers](#) on page 141

[Manage database servers](#) on page 142

Distributed ESM (DESM) settings

Distributed ESM (DESM) provides a distributed architecture that allows a parent ESM to connect to and gather data from up to 100 devices. You can also seamlessly drill down to data that originated and remains on the device ESM.

If you log on with administrator rights to the DESM, a notification appears stating, "This ESM has been added as a Distributed ESM on another server. Waiting for approval to connect." When you click **Approve Hierarchical ESMs**, you can select the type of communication the parent ESM can have with the DESM.

When keying a distributed ESM after changing the IP address of the child, port 443 must be open to reconnect with the ESM.

The parent ESM

The parent pulls data from the device based on filters that you define. The DESM must approve the parent ESM to allow it to pull events. The parent can set filters, sync data sources, and push its custom types. It can't get rules or events from the DESM until it is approved.

The parent ESM doesn't manage devices belonging to the device ESM. The parent ESM shows the System Tree of the device ESM to which it is directly connected. It does not pull events from or display any of the devices' child ESM. Toolbars are disabled for all DESM children.

The parent does not manage data that resides on the device ESM. Instead, a subset of the device from the ESM data is transferred and stored on the parent ESM, based on the filters you define.

Add DESM filters

Data transferred from the device ESM to the parent DESM depend on user-defined filters. When these filters are saved, it's equivalent to applying the filter on the device ESM, so the appropriate hashes or bitsets can be generated. Because the purpose of the DESM feature is to allow you to gather specific data from the device ESM (not ALL data), you must set filters for data to be retrieved from the device ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **DESM Properties**, then click **Filters**.
- 2 Enter the requested data, then click **OK**.

ePolicy Orchestrator settings

You can add an ePolicy Orchestrator device to the ESM, with its applications listed as children on the system navigation tree. Once authenticated, you can access functions from the ESM, and assign ePolicy Orchestrator tags to source or destination IP addresses directly and to events generated by alarms.

You must associate the ePolicy Orchestrator with a Receiver because the events are pulled from the Receiver, not ePolicy Orchestrator.



You must have read permissions on the master database and ePolicy Orchestrator database to use ePolicy Orchestrator.

If the McAfee ePO device has a McAfee® Threat Intelligence Exchange (TIE) server, it is added automatically when you add the McAfee ePO device to the ESM (see *Threat Intelligence Exchange integration*).

Launch ePolicy Orchestrator

If you have an ePolicy Orchestrator device or data source on the ESM, and the ePolicy Orchestrator IP address is on your Local Network, you can launch the ePolicy Orchestrator interface from the ESM.

Before you begin

Add an ePolicy Orchestrator device or data source to the ESM.




This feature is available on ePolicy Orchestrator 4.6 and later.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select a view.
- 2 Select a result from a bar, list, pie, graph, or table component that returns source IP or destination IP data.

- 3 On the component's menu , click **Action | Launch ePO**.
- If you only have one ePolicy Orchestrator device or data source on the system and you selected a source IP or destination IP in Step 1, ePolicy Orchestrator launches.
 - If you have more than one ePolicy Orchestrator device or data source on the system, select the one you want to access and ePolicy Orchestrator launches.
 - If you selected an event or flow on a table component in Step 1, select whether you want to access the source IP or destination IP address, then ePolicy Orchestrator launches.

McAfee ePO device authentication

Authentication is required before using McAfee ePO tagging or actions.

There are two types of authentication:

- Single global account — If you belong to a group that has access to a McAfee ePO device, you can use these features after entering the global credentials.
- Separate account for each device per user — You need privileges to view the device in the device tree.

When you use actions or tags, use the selected method of authentication. If the credentials aren't found or are invalid, you are prompted to enter valid credentials, which you must save for future communication with the device.

Setting up separate account authentication

Global account authentication is the default setting. There are two things you must do to set up separate account authentication.

- 1 Verify that **Require user authentication** is selected when adding the McAfee ePO device to the ESM or when you set up its connection settings (see *Add devices to the ESM console* or *Change connection with ESM*).
- 2 Enter your credentials on the **Options** page (see *Add McAfee ePO authentication credentials*).

Add McAfee ePO authentication credentials

Before using McAfee ePO tagging or actions, you must add the authentication credentials to the ESM.

Before you begin

Install a McAfee ePO device on the ESM (see *Add devices to the ESM console*).

Contact your system administrator if you don't have the user name and password for the device.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation bar of the ESM console, click **options**, then click **ePO Credentials**.
- 2 Click the device, then click **Edit**.
- 3 Provide the user name and password, then click **Test Connection**.
- 4 Click **OK**.

Assign ePolicy Orchestrator tags to IP address

The **ePO Tagging** tab lists the available tags. You can assign tags to events generated by an alarm and view if an alarm has ePolicy Orchestrator tags. You can also select one or more tags on this page and apply them to an IP address.



To access the tagging functionality, you must have the **Apply, exclude, and clear tags** and **Wake up agents; view Agent Activity Log** permissions on ePolicy Orchestrator.


Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **ePO Properties**, then click **Tagging**.
- 2 Complete the requested information, then click **Assign**.

The selected tags are applied to the IP address.

Table 3-83 Option definitions

Option	Definition
Tagging table	Lists the tags available on the device.
IP address to assign...	Type a host name or IP address (supports comma delimited list), then select one or more tags on the Tags list. <div> In order to access the tagging functionality, you must have the Apply, exclude, and clear tags and Wake up agents; view Agent Activity Log permissions.</div>
Wake up Client	Select to wake up the application to apply the tags immediately.
Assign	Click to apply the selected tags to the IP address.

McAfee Risk Advisor data acquisition

You can specify multiple ePolicy Orchestrator servers from which to acquire the McAfee Risk Advisor data. The data is acquired through a database query from the ePolicy Orchestrator SQL Server database.

The database query results in an IP versus reputation score list, and constant values for the low reputation and high reputation values are provided. All ePolicy Orchestrator and McAfee Risk Advisor lists are merged, with any duplicate IPs getting the highest score. This merged list is sent, with low and high values, to any ACE devices used for scoring SrcIP and DstIP fields.

When you add ePolicy Orchestrator, you are asked if you want to configure McAfee Risk Advisor data. If you click **Yes**, a data enrichment source and two ACE scoring rules (if applicable) are created and rolled out. To view these, go to the **Data Enrichment** and **Risk Correlation Scoring** pages. If you want to use the scoring rules, you must create a risk correlation manager.

Enable McAfee Risk Advisor data acquisition

When you enable McAfee Risk Advisor data acquisition on ePolicy Orchestrator, a score list is generated and sent to any ACE device to be used for scoring SrcIP and DstIP fields.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **ePO Properties | Device Management**, then click **Enable**.

You are informed when acquisition is enabled.

2 Click OK.

Table 3-84 Option definitions

Option	Definition
Manage ELM Logging	Configure the default logging pool for the selected device (see <i>Set default logging pool</i>). This option is only available if you have an ELM on the ESM.
Zone	Assign the McAfee ePO to a zone or change the current setting (see <i>Zone Management</i>).
Manual refresh device	Refresh the list of applications from your McAfee ePO device and build a client data source for each application.
Last Refresh Time	View the last time the applications were refreshed.
Enable MRA	Enable McAfee Risk Advisor data acquisition (see <i>McAfee Risk Advisor data acquisition</i>).
Priority	<p>You might have more than one McAfee ePO device, asset source, or vulnerability assessment device set up to receive the same assets or threats. If you do, select the priority that the information from this McAfee ePO device should have if the same information is received by the devices.</p> <p>For example, your computer is being monitored by ePO-1 and VA-1. ePO-1 collects software and hardware information from your computer and VA-1 collects the fact that your computer has Windows installed. Set ePO-1 to have higher priority than VA-1, so the information it collects can't be overwritten by the information VA-1 collects.</p>
Schedule application refresh	To automatically refresh the list of applications from your ePolicy Orchestrator device, select the frequency from the drop-down list.

Threat Intelligence Exchange integration

Threat Intelligence Exchange verifies the reputation of executable programs on the endpoints connected to these files.

When you add a McAfee ePO device to the ESM, the system automatically detects if a Threat Intelligence Exchange server is connected to the device. If it is, the ESM starts listening in on the DXL and logging events.



You might experience a time delay when the ESM connects to the DXL.

When the Threat Intelligence Exchange server is detected, Threat Intelligence Exchange watchlists, data enrichment, and correlation rules are added automatically and Threat Intelligence Exchange alarms are enabled. You receive a visual notification, which includes a link to the summary of the changes made. You are also notified if the Threat Intelligence Exchange server is added to the McAfee ePO server after the device has been added to the ESM.

Once Threat Intelligence Exchange events are generated, you can view their execution history (see *View Threat Intelligence Exchange execution history and set up actions*) and select the actions you want to take on the malicious data.

Correlation rules

Six correlation rules are optimized for Threat Intelligence Exchange data. They generate events that you can search and sort through.

- TIE — GTI reputation changed from clean to dirty
- TIE — Malicious file (SHA-1) found on increasing number of hosts
- TIE — Malicious file name found on increasing number of hosts
- TIE — Multiple malicious files found on single host
- TIE — TIE reputation changed from clean to dirty
- TIE — Increase in malicious files found across all hosts

Alarms

The ESM has two alarms that might trigger when important Threat Intelligence Exchange events are detected.

- **TIE bad file threshold exceeded** triggers from the correlation rule **TIE - Malicious file (SHA-1) found on increasing number of hosts**.
- **TIE unknown file executed** triggers from a specific TIE event and adds information to the **TIE data source IPs** watchlist.

Watchlist

The **TIE data source IPs** watchlist maintains a list of systems that have triggered the **TIE unknown file executed** alarm. It is a static watchlist with no expiration.

Threat Intelligence Exchange execution history

You can view the execution history for any Threat Intelligence Exchange event (see *View Threat Intelligence Exchange execution history and set up actions*), which includes a list of the IP addresses that have attempted to execute the file. On this page, you can select an item and take any of these actions:

- Create a watchlist.
- Append the information to a watchlist.
- Create an alarm.
- Add the information to a blacklist.
- Export the information to a .csv file.

See also

[View Threat Intelligence Exchange execution history and set up actions on page 149](#)

View Threat Intelligence Exchange execution history and set up actions


The Threat Intelligence Exchange execution history page displays a list of systems that have executed the file associated with the event you selected.

Before you begin

An ePolicy Orchestrator device with an attached Threat Intelligence Exchange server on the ESM must exist.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree of the ESM console, click the ePolicy Orchestrator device.
- 2 On the views drop-down list, select **Event Views | Event Analysis**, then click the event.
- 3 Click the menu icon , then select **Actions | TIE Execution History**.
- 4 On the **TIE Execution History** page, view the systems that have executed the Threat Intelligence Exchange file.
- 5 To add this data to your workflow, click a system, click the **Actions** drop-down menu, then select an option to open its ESM page.
- 6 Set up the action you selected (see the online Help for instructions).

See also

[Threat Intelligence Exchange integration on page 148](#)

Query McAfee ePO devices for a report or view


You can query multiple McAfee ePO devices for a report or view if they are integrated with McAfee Real Time for McAfee ePO.

Before you begin

Verify that McAfee ePO devices to be queried are integrated with McAfee Real Time for McAfee ePO.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click the system, click the **Properties** icon , then click **Reports**.
- 2 Click **Add**, fill out sections 1 through 4, then click **Add** in section 5.
- 3 On the **Report Layout** editor, drag and drop a **Table**, **Bar Chart**, or **Pie Chart** component.
- 4 On the **Query Wizard**, select **Real Time for McAfee EPO** on the drop-down list, , then select the element or question for the query.
- 5 Click **Next**, click **Devices**, then select the McAfee ePO devices to be queried.
- 6 (Optional) Click **Filters**, add filter values for the query, then click **OK**.
- 7 If you selected **Custom ePO Question** on the drop-down list, click **Fields**, select the elements that you want to include in the question, then click **OK**.
- 8 Click **Finish** to close the **Query Wizard**, define the properties in the **Properties** pane, then save the report.

Query McAfee ePO devices for data enrichment


You can query multiple McAfee ePO devices for data enrichment if they are integrated with McAfee Real Time for McAfee ePO.

Before you begin

Verify that McAfee ePO devices to be queried are integrated with McAfee Real Time for McAfee ePO.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system, click the **Properties** icon , then click **Data Enrichment**.
- 2 Click **Add**, type a name, then make the selections on the **Main** tab.
- 3 On the **Source** tab, select McAfee Real Time for McAfee ePO in the **Type** field, then select the devices in the **Device** field.
- 4 Set the remaining settings on the **Query**, **Scoring**, and **Destination** tabs, then click **Finish**.

McAfee Vulnerability Manager settings

The McAfee Vulnerability Manager can be added to the ESM as a device, allowing you to start a scan on the McAfee Vulnerability Manager from the ESM. This is useful if you purchased a McAfee Vulnerability Manager device and want to run it from the ESM.

McAfee Vulnerability Manager must be associated with a Receiver because the events are pulled from the Receiver, not the McAfee Vulnerability Manager.

See also

[Obtain McAfee Vulnerability Manager certificate and passphrase on page 151](#)

[Run McAfee Vulnerability Manager scans on page 151](#)

[Set up McAfee Vulnerability Manager connection on page 152](#)

Obtain McAfee Vulnerability Manager certificate and passphrase

You must obtain the McAfee Vulnerability Manager certificate and passphrase before setting up McAfee Vulnerability Manager connections. This task is not performed on the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the server that is running Foundstone Certificate Manager, run Foundstone Certificate Manager.exe.
- 2 Click the **Create SSL Certificates** tab.
- 3 In the **Host Address** field, type the host name or IP address for the system hosting the web interface for McAfee Vulnerability Manager, then click **Resolve**.
- 4 Click **Create Certificate using Common Name** to generate the passphrase and a .zip file.
- 5 Upload the .zip file and copy the passphrase that was generated.

See also

[McAfee Vulnerability Manager settings on page 150](#)

[Run McAfee Vulnerability Manager scans on page 151](#)

[Set up McAfee Vulnerability Manager connection on page 152](#)

Run McAfee Vulnerability Manager scans

The **Scans** page shows all the vulnerability scans that are running or have run from McAfee Vulnerability Manager, and their status. When you open this page, an API checks if there are default web login credentials. If there are, the scan list is populated based on those credentials, and is updated every 60 seconds. You can initiate a new scan from this page as well.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **MVM Properties**, then click **Scans**.
- 2 Click **New Scan** and enter the information requested.
- 3 Click **OK**.

When the scan is complete it's added to the list of scans.

See also

[McAfee Vulnerability Manager settings on page 150](#)

[Obtain McAfee Vulnerability Manager certificate and passphrase on page 151](#)

[Set up McAfee Vulnerability Manager connection on page 152](#)

Set up McAfee Vulnerability Manager connection

You must set up McAfee Vulnerability Manager connections to the database to pull the vulnerability assessment data from McAfee Vulnerability Manager, and to the web user interface to perform scans on McAfee Vulnerability Manager.

Before you begin

You must obtain the McAfee Vulnerability Manager certificate and passphrase

Changing these settings doesn't affect the device itself. It only affects the way the device communicates with the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **MVM Properties**, then click **Connection**.
- 2 Fill in the information requested, then click **OK**.

See also

[McAfee Vulnerability Manager settings on page 150](#)

[Obtain McAfee Vulnerability Manager certificate and passphrase on page 151](#)

[Run McAfee Vulnerability Manager scans on page 151](#)

McAfee Network Security Manager settings

The McAfee Network Security Manager can be added to the ESM as a device, allowing you to access the functions from the ESM. This is useful if you purchased a device and want to access it from the ESM.

When you add a McAfee Network Security Manager device to the ESM, the sensors on the device are listed as children under the device on the system navigation tree. The device must be associated with a Receiver because the events are pulled from the Receiver, not the McAfee Network Security Manager.

See also

[Add a blacklist entry on page 152](#)

[Add or delete a removed blacklist entry on page 153](#)

[Layer 7 collection on an NSM device on page 153](#)

Add a blacklist entry

The McAfee Network Security Manager applies blacklisting through the sensors. The **Blacklist** page displays the blacklist entries that were defined for the sensor that you select. From this page, you can add, edit, and delete blacklist items.



You must be a super user to use the blacklist function.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **NSM Properties**, click **Blacklist**, then select a sensor.
- 2 To apply the global blacklist entries to this sensor, select **Include Global Blacklist**.

The global blacklist item is added to the list. If there are duplicate IP addresses, the global blacklist address overwrites the McAfee Network Security Manager address.



Once you select this option, it can't be undone automatically. Delete items manually.

- 3 Click **Add**, fill in the information requested, then click **OK**.

The entry appears on the blacklist until its duration expires.

Table 3-85 Option definitions

Option	Definition
IP Address	Type the IP address you want to blacklist.
Duration	Select the length of time you want this address on the blacklist.
Description	Type a description of this entry.

See also

[McAfee Network Security Manager settings on page 152](#)

[Add or delete a removed blacklist entry on page 153](#)

[Layer 7 collection on an NSM device on page 153](#)

Add or delete a removed blacklist entry

Any entry that was initiated on the ESM with a duration that hasn't expired, but is not returned on the list of blacklist entries when the McAfee Network Security Manager (Manager) is queried, is displayed with a **Removed** status and a flag icon.

This condition occurs if the entry was removed, but the removal was not initiated on the ESM. You can re-add this entry to or delete it from the blacklist.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **NSM Properties**, then click **Blacklist**.
- 2 Select the removed entry on the list of blacklist entries, then click **Add** or **Delete**.
- 3 Click **Apply** or **OK**.

See also

[McAfee Network Security Manager settings on page 152](#)

[Add a blacklist entry on page 152](#)

[Layer 7 collection on an NSM device on page 153](#)

Layer 7 collection on an NSM device

Layer 7 data is populated in the NSM database after the NSM event is written to its database. It doesn't come into the system as part of the event.

To pull Layer 7 information from the NSM, you can delay when the event is pulled so that Layer 7 data is included. This delay applies to all NSM events, not only the ones with associated Layer 7 data.

You can set this delay when performing three different actions related to the NSM:

- Adding a McAfee NSM device to the console
- Configuring an NSM device
- Adding an NSM data source

Adding a McAfee NSM device

When adding the NSM device to the ESM (see *Add devices to the ESM console*), select **Enable Layer 7 Collection** and set the delay on the fourth page of the **Add Device Wizard**.

Configuring an NSM device

After adding an NSM device to the ESM console, you can configure the connection settings for the device (see **Change connection with ESM**). You can select **Enable Layer 7 Collection** and set the delay on the **Connection** page.

Adding an NSM data source

To add an NSM data source to a Receiver (see *Add a data source*), select McAfee in the **Data Source Vendor** field and **Network Security Manager - SQL Pull (ASP)** in the **Data Source Model** field. You can select **Enable Layer 7 Collection** and set the delay on the **Add Data Source** page.

See also

McAfee Network Security Manager settings on page 152

Add a blacklist entry on page 152

Add or delete a removed blacklist entry on page 153

Configuring ancillary services

Ancillary services include Remedy servers, Network Time Protocol (NTP) servers, and DNS servers. Configure these servers to communicate with ESM.

Contents

- *General system information*
- *Configure Remedy server settings*
- *Stop automatic refresh of ESM system tree*
- *Defining message settings*
- *Set up NTP on a device*
- *Manage Global Blacklists page*
- *Configure network settings*
- *System time synchronization*
- *Install a new certificate*
- *Configure profiles*
- *SNMP configuration*

General system information

On the **System Properties** | **System Information** page, you can see general information about your system and the status of various functions. On the **System Log** page, you can see events that have taken place on the system or devices.

You can refer to this information when you speak with McAfee support about your system. You also need it when you are setting up features such as event or flow aggregation, or to check on the status of a rules update or system backup.

- **System, Customer ID, Hardware, and Serial Number** provide information about the system and its current status.
- **Database Status** shows when the database is performing other functions (for example, a database rebuild or background rebuild) and the status of those functions. An **OK** status means that the database is operating normally.
- **System Clock** shows the date and time that **System Properties** was last opened or refreshed.
- **Rules Update** shows the last time the rules were updated.
- When in FIPS mode, **FIPS self-test** and **Status** show the last time a FIPS self-test was performed and its status.
- **View Reports** shows the **Device Type Count** and **Event Time** reports.

Table 3-86 Option definitions

Option	Definition
System	The device type, the software version and build number, and the machine ID number, which is a unique number assigned to each device.
Customer ID	The number that you are given when you set up your permanent credentials with McAfee.
Hardware	Information about the hardware and memory.
Serial Number	The manufacturer's serial number for this device.
System Clock (GMT)	The date and time the System Properties page was last opened or refreshed. If you click the link, you can change the system clock and NTP settings.
Sync Device Clocks	Syncs the ESM time and NTP servers to the devices.
Rules Update	The last time the rules were updated and how they were updated. If you haven't set up your permanent credentials, it shows when your license expires (see <i>Check for rule updates</i> or <i>Obtain rule download credentials</i>).
Database Status	The status of the database. If it is performing a function such as a database or background rebuild, it displays the status of that function. An OK status means it is operating normally.
Refresh System Information	Refreshes the data displayed on the page.
Device Summary Reports	Shows the Device Type Count and Event Time reports. You can export this data to a .csv file.

Configure Remedy server settings

If you have a Remedy system set up, you must configure the remedy settings so the ESM can communicate with it.

Before you begin

Set up your Remedy system.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Custom Settings | Remedy**.
- 2 On the **Remedy Configuration** page, enter the information for your Remedy system, then click **OK**.

When you select **Send event to Remedy**  on the **Event Analysis** view, the email is populated with the information that you entered on this page.

Table 3-87 Option definitions

Option	Definition
Host	Type the host for your Remedy system.
Port	Change the port number, if needed.
Use TLS	Select if you want to use TLS as the encryption protocol
Username	Type the user name for the Remedy system, if one is required.
Password	Type the password for the Remedy system, if one is required.
From Address	Type the email address of the remedy message sender.
To Address	Type the email address where the remedy message is sent.

Stop automatic refresh of ESM system tree

The ESMsystem tree is refreshed automatically every five minutes. You can stop the automatic refresh if needed.


Before you begin


You must have **System Management** rights to change this setting.

During the refresh, you can't select devices on the tree. If you have many devices on the ESM, this can interfere with accessing the **Properties** page for the devices.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system tree, select the ESM, then click the **Properties** icon .
- 2 Click **Custom Settings**, then deselect **Automatic refresh of the System Tree**.

You can refresh the system tree manually by clicking the **Refresh Devices** icon  on the system tree actions toolbar.

Defining message settings

When you define alarm actions or set up report delivery methods, you can choose to send messages. But first, you must connect ESM to your mail server and identify message recipients via email, SMS, SNMP, or syslog.

ESM sends alarm notifications using the SNMP v1 protocol. SNMP uses User Datagram Protocol (UDP) as the transport protocol for passing data between managers and agents. In an SNMP setup, agents, such as ESM, forward events to SNMP servers (referred to as Network Management Station [NMS]), using packets of data known as *traps*. Other agents in the network can receive event reports the same way they receive notifications. Due to size limitations of SNMP trap packets, ESM sends each report line in a separate trap.

Syslog can also send query CSV reports generated by the ESM. Syslog sends these query CSV reports one line per syslog message, with the data of each line of the query results arranged in comma-separated fields.

See also

[Connect your mail server on page 157](#)

[Manage recipients on page 157](#)

[Manage email recipient groups on page 158](#)

[Create alarm message templates on page 240](#)

[Set up correlation alarms to include source events on page 241](#)

[Manage alarm recipients on page 243](#)

Connect your mail server


Configure the settings to connect to your mail server to deliver alarm and report messages.

Before you begin

Verify that you have administrator rights or belong to an access group with user management privileges.

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Email Settings**, and enter the requested information to connect your mail server.

Option	Description
Host and Port	Enter the host and port for your mail server.
Use TLS	Select whether to use the TLS encryption protocol.
User name and Password	Type the user name and password to access your mail server.
Title	Type a generic title for all email messages sent from your mail server, such as the ESM IP address to identify which ESM generated the message.
From	Type your name.
Configure Recipients	Add, edit, or remove recipients (see Manage alarm recipients on page 243)

- 3 Send a test email to verify the settings.
- 4 Add, edit, or remove recipients (see [Manage alarm recipients on page 243](#))
- 5 Click **Apply** or **OK** to save the settings.

See also

[Defining message settings on page 156](#)

[Manage recipients on page 157](#)

[Manage email recipient groups on page 158](#)

Manage recipients

Alarm or report messages can be sent in several formats, each of which has a list of recipients that you can manage. Email addresses can be grouped so you can send a message to several recipients at once.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Email Settings**.
- 2 Click **Configure Recipients**, then select the tab you want to add them to.
- 3 Click **Add**, then add the requested information.
- 4 Click **OK**.

The recipient is added to the ESM and you can select them anywhere recipients are used throughout the ESM.

See also

[Defining message settings on page 156](#)

[Connect your mail server on page 157](#)

[Manage email recipient groups on page 158](#)

Manage email recipient groups


Group email recipients so that you can send a message to several recipients at one time.

Before you begin

Recipients and their email addresses must be defined for users in the ESM (see *Add a user*).

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click the system, then click the **Properties** icon .
- 2 Click **Email Settings**, then click **Configure Recipients | Email Groups**.
You see a list of existing email recipient groups and the members of the selected group.
- 3 Click **Add**, **Edit**, or **Remove** to manage the list of recipients groups.
- 4 Provide the information requested, then click **OK**.

The group is added to the **Email Recipients Groups** section of the **Email Groups** page.

Table 3-88 Option definitions

Option	Definition
E-mail Group Name	Type a name that describes the group.
Select e-mail addresses	From the list of all recipients on the system, select the ones to be part of this group.

See also

[Defining message settings on page 156](#)

[Connect your mail server on page 157](#)

[Manage recipients on page 157](#)

Set up NTP on a device

Synchronize the device time with the ESM using a Network Time Protocol (NTP) server.

Task

For details about product features, usage, and best practices, click ? or **Help**.



- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Configuration | NTP**.
- 3 Fill in the information requested, then click **OK**.

Table 3-89 Option definitions

Option	Definition
Use NTP Server(s) for time synchronization	Select this option to use NTP servers to synchronize the device's time instead of using the system clock.
Table	View the default NTP servers and any that have been added to the device.
NTP Server column	Add IP addresses for NTP servers that you want to add to the device by clicking in this column. You can add up to 10 servers. <div> NTP server addresses on IPS class devices must be IP addresses.</div>
Authentication Key and Key ID columns	Type the authentication key and key ID for each NTP server (contact your network administrator if you do not know them).
Status	Click to view the status of the NTP servers on the list. If you have made changes to the list of servers, you must click OK to save the changes and close the page, then open the page again before clicking Status .

Tasks

- [View status of NTP servers on page 159](#)
View the status of all the NTP servers on the ESM.

See also

[View status of NTP servers on page 159](#)

View status of NTP servers

View the status of all the NTP servers on the ESM.

Before you begin

Add NTP servers to the ESM or devices (see *System time synchronization* or *Set up NTP on a device*).

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, do one of the following:
 - Select **System Properties | System Information**, then click **System Clock**.
 - On the system navigation tree, select a device, click the **Properties** icon, then select **Configuration | NTP**.
- 2 Click **Status**, view the NTP server data, then click **Close**.

Table 3-90 Option definitions

Option	Definition
NTP Server column	Lists the IP addresses for the NTP servers. These markings might appear before the address: <ul style="list-style-type: none"> • * – Server currently being referenced • + – Selected, included in the final set • # – Selected, distance exceeds maximum value • o – Selected, Pulse Per Second (PPS) used • x – Source false ticker • . – Selected from end of candidate list • - – Discarded by cluster algorithm
Reachable column	Yes means the server can be reached and no means it can't.
Authentication column	None means no credentials have been provided, Bad means the credentials were incorrect, and yes means the correct credentials were provided.
Condition column	The condition corresponds to the mark in the NTP Server column. Candidate means it is a possible choice, sys.peer means it is the current choice, and reject means it can't be reached. If all servers are marked reject , it's possible that the NTP configuration is restarting.

See also

[Set up NTP on a device on page 158](#)

Manage Global Blacklists page

Select the network devices that support global blacklist.

Table 3-91 Option definitions

Option	Definition
Table	View a list of the network devices on the ESM and whether or not global blacklist is enabled on each of them.
Enabled column	Select the devices that use global blacklist.

Configure network settings

Configure the way ESM connects to your network by adding ESM server gateway and DNS server IP addresses, defining proxy server settings, setting up SSH, and adding static routes.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Network Settings**.
- 2 Fill in the information to configure the connection to your network.
- 3 Click **Apply** or **OK**.

Table 3-92 Option definitions



Tab	Option	Definition
Main	Interface 1 and Interface 2	<p>Select Interface 1, Interface 2, or both, then click Setup. At least one interface must always be enabled.</p> <div>  <p>Firefox versions 4 and 5 currently are unable to remove "[]" from the address while verifying the certificate, so they can't resolve IPv6 addresses while trying to get the certificates over IPv6. To work around this issue, add a record for the IPv6 address in the /etc/hosts file (Linux) or C:\WINDOWS\system32\drivers\etc\hosts (Windows) and use the host name instead of the IPv6 address to navigate to the ESM.</p> </div>
	Enable SSH (not available in FIPS mode)	<p>Select this to allow SSH connections. At least one interface must be defined to enable SSH.</p> <div>  <p>ESM and devices use a FIPS capable version of SSH. SSH clients OpenSSH, Putty, dropbear, Cygwin ssh, WinSCP and TeraTerm have been tested and are known to work. If you are using Putty, version 0.62 is compatible and you can download it at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.</p> </div>
	SSH Port	Enter the specific port that access is allowed through.
	Manage SSH keys	Click SSH Keys . If you have enabled SSH connections, the machine(s) listed communicates. To discontinue communication, delete the machine ID from the list.
	IPv6 Settings	<p>Select Manual or Auto to enable IPv6 mode.</p> <ul style="list-style-type: none"> If the setting is Off, IPv6 mode is disabled. If you select Auto, the Primary and Secondary IPv6 fields are disabled. Each host determines its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address. If you select Manual, the Primary and Secondary IPv6 fields are enabled. Add the IPv6 addresses in these fields.
Advanced	Set up Internet Control Message Protocol (ICMP) messages and the Intelligent Platform Management Interface (IPMI) on the ESM or its devices.	
	ICMP Messages	<p>Select any of the following options for ICMP:</p> <ul style="list-style-type: none"> Redirects — The ESM ignores redirect messages. Dest Unreachable — The ESM generates a message when a packet can't be delivered to its destination for reasons other than congestion. Enable PING — The ESM sends an <i>Echo Reply</i> message in response to an <i>Echo Request</i> message sent to an IPv6 multicast/anycast address.
	IPMI Settings	<p>If you have an IPMI NIC plugged into a switch and you need to remotely manage the ESM devices through an IPMI card, add the IPMI settings:</p> <ul style="list-style-type: none"> Enable IPMI Settings — Select to have access to IPMI commands. VLAN, IP Address, Netmask, Gateway — Enter the settings to configure the network for the IPMI port.
Proxy	If your network uses a proxy server, set up the connection to your ESM.	
	IPv4 or IPv6	On devices, if you have an interface that is using an IPv6 address, you can select IPv6. If not, IPv4 is selected.

Table 3-92 Option definitions *(continued)*

Tab	Option	Definition
Traffic	IP Address, Port, Username, Password	Enter the information required to connect to the proxy server.
	Basic Authentication	Select to implement basic authentication checking.
	Define a maximum data output value for a network and mask to control the rate at which outbound traffic is sent.	
	Table	View the existing controls that you have set up.
	Network column	View the addresses of the networks that the system controls outbound traffic on, based on what you have defined.
	Mask column	(Optional) View the masks for the network addresses.
Static Routes	Maximum Throughput column	View the maximum throughput you defined for each network.
	Add, Edit, Delete	Manage the network addresses that you want to control.
	Static Routes	Add, edit, or remove static routes. A static route is a specified set of instructions regarding how to reach a host or network not available through the default gateway. When you add a static route, the change is pushed to the ESM and immediately takes effect when you click Apply . Upon applying changes, the ESM re-initializes itself, causing all current sessions to be lost.

Table 3-93 Option definitions

Option	Definition
IPv4 or IPv6 (not available on all Proxy tabs)	If you have an interface that is using an IPv6 address, you can select IPv6. If not, IPv4 is selected.
IP Address, Port, Username, Password	Enter the information required to connect to the proxy server.
Basic Authentication	Select to implement basic authentication checking.

Table 3-94 Option definitions on the Network tab


Option	Definition
Bypass NIC Configuration	Set bypass NIC so that the device passes all traffic, even if it is malicious (see <i>Set up bypass NICs</i>). Devices in IDS mode do not have bypass capabilities, so their status is Normal Operation .
Collect Flows	(Optional) Select to collect flows for traffic sent to and from the device.
ELM EDS SFTP	<p>If you have ELM SFTP Access user privileges, you can view and download ELM log files stored for the devices. If you have Device Management privileges, you can change the port to access these files in the ELM EDS SFTP field. Do not use these ports: 1, 22, 111, 161, 695, 1333, 1334, 10617, or 13666.</p> <div>  <p>We recommend that you use this feature with one of the following FTP clients: WinSCP 5.11, Filezilla, CoreFTP LE, or FireFTP.</p> </div>
HOME_NET	Type IP addresses, owned by your organization, that determine the direction of the flow traffic that the device is collecting.

Table 3-94 Option definitions on the Network tab *(continued)*

Option	Definition
Interfaces	<p>Select the interfaces to be used and enter the IP addresses for the IPv4 or IPv6 type. If you enter an IPv4 address, add the netmask address as well. If you enter an IPv6 address, include the netmask in the address or you receive an error.</p> <p>To allow the device to be used from multiple networks (limited to MGT 1 <primary interface> and MGT 2 <first drop-down interface> only), add more interfaces.</p> <p>To activate NIC bonding, select Management in the first field, then type the same IP address and netmask as the main NIC (first line on this dialog box).</p>
IPv6 Mode	<p>Select whether to enable IPv6 mode.</p> <ul style="list-style-type: none"> • Off: IPv6 mode is not enabled. The IPv6 fields are disabled. • Auto: IPv6 mode is enabled. Each host determines its address from the contents of received user advertisements. It uses the IEEE EUI-64 standard to define the network ID portion of the address. The IPv6 fields are disabled. • Manual: IPv6 mode is enabled. The IPv6 fields are enabled.
SSH Port	Select the port through which access is allowed between the ESM and the device.

Table 3-95 Option definitions





Option	Definition
DHCP	<p>If you are not working in the cloud environment, select to enable DHCP services. DHCP is useful if you need to reset the IP addresses for your network.</p> <div>  If you are using a redundant ESM or ELM, redundancy stops working if the IP address of the redundant device is changed. </div>
IPv4 , Netmask, IPv6	<p>Type IP addresses and a netmask for IPv4.</p> <div>  Firefox versions 4 and 5 currently are unable to remove "[]" from the address while verifying the certificate, so they can't resolve IPv6 addresses while trying to get the certificates over IPv6. To work around this issue, add a record for the IPv6 address in the /etc/hosts file (Linux) or C:\WINDOWS\system32\drivers\etc\hosts (Windows) and use the host name instead of the IPv6 address to navigate to the ESM. </div>
Gateway	Enter the gateway that works with your network configuration. It must be an IPv4 address.
DNS Server 1 and 2	Specify at least one DNS server. Without a DNS server, the ESM can't check for signatures and software updates from McAfee servers. Features such as emails and WHOIS are also unavailable without a valid DNS server. These are AND/OR fields for IPv4 and IPv6 addresses. You must have an IPv6 address defined in Interface 1 or 2 to use it as a DNS server address.
Configure VLANs and Aliases	<p>Click Advanced.</p> <ul style="list-style-type: none"> • If you are using a VLAN, add it to the ESM. • If you have more than one IP address for a network device, add an alias.

Table 3-96 Option definitions for Communication tab on Receiver device

Option	Definition
SNMP Port, Syslog Port, sFlow Port	<p>Select the port that the firewall on the Receiver opens up to, so it can listen for inbound protocol data source information. A port of 0 means collection is turned off.</p> <p> The Receiver performs UDP and TCP syslog collection.</p>
Syslog TLS Port	<p>Select the port that the firewall on the Receiver opens up to, so it can listen for inbound TLS protocol data source information. The default port is 10514. A port of 0 means that TLS syslog collection is turned off. When you add a data source, you can specify that you only want syslog TLS accepted from the data source if this port is enabled. TLS supports only self-signed certificates.</p>
MEF Port	<p>Select the port that the firewall on the Receiver opens up to, so it can listen for inbound MEF data source information. The default port is 8081. A port of 0 means that MEF collection is turned off.</p> <p> All MEF data sources with the same IP address must be marked as encrypted or unencrypted.</p>
IPFIX Port	<p>Select the port that the firewall on the Receiver opens up to, so it can listen for inbound IPFIX protocol data source information. The default port is 4739. A port of 0, which is the default, and means that IPFIX collection is turned off.</p>
NetFlow Ports	<p>Select the ports that the firewall on the Receiver opens up to, so it can listen for inbound NetFlow protocol data source information. This list can contain multiple ports that are comma-separated. A blank value in this field means that NetFlow collection is turned off.</p>
DHCP address	<p>A range of DHCP IP addresses, which enables the collection of logs sent to the Event Receiver from DHCP data sources within this range. A DHCP data source can be any data format that is supported and sent to the Receiver via the McAfee Labs Windows Event Collector.</p>

Tasks

- [Set up the IPMI port on ESM or devices on page 168](#)
Configure the network for the IPMI port to set up IPMI on the ESM or its devices.
- [Set up network traffic control on the ESM on page 170](#)
Define a maximum data output value for the ESM.
- [Set up DHCP on page 174](#)
Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
- [Set up DHCP on VLAN on page 174](#)
Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

Managing network interfaces

Communication with a device can take place using the public and private interfaces of the traffic paths. This means that the device is invisible in the network because it doesn't require an IP address.

Management interface

Alternately, network administrators can configure a management interface with an IP address for communication between the ESM and the device. These features of a device require the use of a management interface:

- Full control of bypass network cards
- Use of NTP time synchronization

- Device-generated syslog
- SNMP notifications

Devices are equipped with at least one management interface, which gives the device an IP address. With an IP address, the ESM can access the device directly without directing communication toward another target IP address or host name.



Do not attach the management network interface to a public network because it's visible to the public network and its security could be compromised.

ESM interface bonding

The ESM tries to auto-enable bonded NIC mode when it detects two management interfaces that are both using the same IP address. When bonded mode is enabled, both interfaces are assigned the same IP address and MAC address. The bonding mode used is mode 0 (round-robin), which provides fault tolerance.

To disable NIC bonding, change the IP address of one of the interfaces so that it no longer matches the other. The system then automatically disables bonded NIC mode.

See also

[Set up network interfaces on page 165](#)

[Add VLANs and aliases on page 167](#)


[Add static routes on page 167](#)

Set up network interfaces

Interface settings determine how the ESM connects to the device. You must define these for each device.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click the device's **Configuration** option, then click **Interfaces**.
- 3 Enter the data as requested, then click **Apply**.

All changes are pushed to the device and take effect immediately. Upon applying changes, the device reinitializes, causing all current sessions to be lost.

Table 3-97 Option definitions on the Network tab


Option	Definition
Bypass NIC Configuration	Set bypass NIC so that the device passes all traffic, even if it is malicious (see <i>Set up bypass NICs</i>). Devices in IDS mode do not have bypass capabilities, so their status is Normal Operation .
Collect Flows	(Optional) Select to collect flows for traffic sent to and from the device.
ELM EDS SFTP	<p>If you have ELM SFTP Access user privileges, you can view and download ELM log files stored for the devices. If you have Device Management privileges, you can change the port to access these files in the ELM EDS SFTP field. Do not use these ports: 1, 22, 111, 161, 695, 1333, 1334, 10617, or 13666.</p> <div> We recommend that you use this feature with one of the following FTP clients: WinSCP 5.11, Filezilla, CoreFTP LE, or FireFTP.</div>
HOME_NET	Type IP addresses, owned by your organization, that determine the direction of the flow traffic that the device is collecting.

Table 3-97 Option definitions on the Network tab (*continued*)

Option	Definition
Interfaces	<p>Select the interfaces to be used and enter the IP addresses for the IPv4 or IPv6 type. If you enter an IPv4 address, add the netmask address as well. If you enter an IPv6 address, include the netmask in the address or you receive an error.</p> <p>To allow the device to be used from multiple networks (limited to MGT 1 <primary interface> and MGT 2 <first drop-down interface> only), add more interfaces.</p> <p>To activate NIC bonding, select Management in the first field, then type the same IP address and netmask as the main NIC (first line on this dialog box).</p>
IPv6 Mode	<p>Select whether to enable IPv6 mode.</p> <ul style="list-style-type: none"> • Off: IPv6 mode is not enabled. The IPv6 fields are disabled. • Auto: IPv6 mode is enabled. Each host determines its address from the contents of received user advertisements. It uses the IEEE EUI-64 standard to define the network ID portion of the address. The IPv6 fields are disabled. • Manual: IPv6 mode is enabled. The IPv6 fields are enabled.
SSH Port	Select the port through which access is allowed between the ESM and the device.

Table 3-98 Option definitions

Option	Definition
ICMP Messages	<p>Select either of the following options for ICMP.</p> <p>Redirect — If selected, the ESM ignores redirect messages.</p> <p>Dest Unreachable — If selected, the ESM generates a message when a packet can't be delivered to its destination for reasons other than congestion.</p> <p>Enable Ping — If selected, the ESM sends an <i>Echo Reply</i> message in response to an <i>Echo Request</i> message sent to an IPv6 multicast/anycast address.</p>
IPMI Settings	<p>To remotely manage the ESM devices through an IPMI card when an IPMI NIC is plugged into a switch, add the IPMI settings.</p> <ul style="list-style-type: none"> • Enable IPMI Settings — Select to have access to IPMI commands. • VLAN, IP Address, Netmask, Gateway — Enter the settings to configure the network for the IPMI port.

Table 3-99 Option definitions

Option	Definition
Add Alias	Highlight the VLAN you want to add the alias to, then click. This option is not available if DHCP is selected.
Add VLAN	Click to add a VLAN to the interface.
Edit	Highlight an alias or VLAN on the table, then click to change its settings.
Delete	Highlight an alias or VLAN on the table, then click to delete it.

See also[Managing network interfaces on page 164](#)[Add VLANs and aliases on page 167](#)[Add static routes on page 167](#)

Add VLANs and aliases

Add Virtual Local Area Networks (VLANs) and aliases to an ACE or ELM interface. Aliases are assigned IP address and netmask pairs that you add if you have a network device with more than one IP address.

Task

For details about product features, usage, and best practices, click ? or **Help**.



- 1 On the system navigation tree, select a device, click the **Properties** icon , then click device **Configuration**.
- 2 In the **Interfaces** section of the **Network** tab, click **Setup**, then click **Advanced**.
- 3 Click **Add VLAN**, enter the information requested, then click **OK**.
- 4 Select the VLAN where you want to add the alias, then click **Add Alias**.
- 5 Enter the requested information, then click **OK**.

Table 3-100 Option definitions

Option	Definition
VLAN	View the VLAN this alias is on. This field is pre-populated with the number of the VLAN this alias is being added to. If it is the Untagged VLAN, this number is 0.
IP Version	Select whether the IP address is in IPv4 or IPv6 format.
IP Address	Type the IP address of the alias.
Netmask	If the address is in IPv4 format, type the netmask.

Table 3-101 Option definitions

Option	Definition
VLAN	Type a number for the VLAN.
DHCP	If you are not working in the cloud environment, select to enable DHCP services. DHCP is useful if you need to reset the IP addresses for your network. <div> If you are using a redundant ESM or ELM, redundancy stops working if the IP address of the redundant device is changed.</div>
IPv4 or IPv6	Select the IP version. IPv4 is selected by default. If you have IPv6 set to Manual or Auto on the Network Settings page, the IPv6 radio button is enabled. Select it if the IP address is in IPv6 format. When selected, the Netmask field is disabled.
IP Address	Type the IP address for the VLAN.
Netmask	If the IP address is in IPv4 format, add the netmask.

See also

[Managing network interfaces on page 164](#)

[Set up network interfaces on page 165](#)

[Add static routes on page 167](#)

Add static routes

A static route is a set of instructions about how to reach a host or network that is not available through the default gateway.

Task

For details about product features, usage, and best practices, click ? or Help.


- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Configuration | Interfaces**.
- 3 Next to the **Static Routes** table, click **Add**.
- 4 Enter the information, then click **OK**.

Table 3-102 Option definitions

Option	Definition
Static Routes table	View the static routes on the system.
Add	Click to add the information for a static route.
Edit	Click to make changes to the settings for the selected static route.
Remove	Click to delete the selected static route.

Table 3-103 Option definitions

Option	Definition
IPv4 or IPv6	Select whether this static route will be looking at IPv4 or IPv6 traffic.
Network and Gateway	Type in the network and gateway IP address for this route.
Mask	Select the mask.

See also

[Managing network interfaces on page 164](#)

[Set up network interfaces on page 165](#)

[Add VLANs and aliases on page 167](#)

IPMI port set up on ESM or devices

You can set up the IPMI port on the ESM or any of its devices.

This enables you to perform several actions:


- Plug the IPMI Network interface controller (NIC) into a switch so that it is available to IPMI software.
- Access an IPMI-based Kernel-based Virtual Machine (KVM).
- Set the IPMI password for the default user after upgrade to ESM 9.4.0.
- Access IPMI commands like power-on and power status.
- Reset the IPMI card.
- Perform a warm and cold reset.

Set up the IPMI port on ESM or devices

Configure the network for the IPMI port to set up IPMI on the ESM or its devices.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the system or any of the devices, then click the **Properties** icon .
- 2 Access the **Network Settings Advanced** tab.
 - On the ESM, click **Network Settings | Advanced**.
 - On a device, click the **Configuration** option for the device, then click **Interfaces | Advanced**
- 3 Select **Enable IPMI Settings**, then type the VLAN, IP address, netmask, and gateway for the IPMI.



If **Enable IPMI Settings** is grayed out on device BIOS, you need to update the system BIOS. SSH to the device and open the `/etc/areca/system_bios_update/Contents-README.txt` file.

- 4 Click **Apply** or **OK**.



If you are upgrading your device, you might receive a message telling you to change the password or re-key the device. If you receive this message, change the system password or re-key the device to set a new password to configure the IPMI.

Table 3-104 Option definitions



Tab	Option	Definition
Main	Interface 1 and Interface 2	<p>Select Interface 1, Interface 2, or both, then click Setup. At least one interface must always be enabled.</p> <div>  <p>Firefox versions 4 and 5 currently are unable to remove "[]" from the address while verifying the certificate, so they can't resolve IPv6 addresses while trying to get the certificates over IPv6. To work around this issue, add a record for the IPv6 address in the <code>/etc/hosts</code> file (Linux) or <code>C:\WINDOWS\system32\drivers\etc\hosts</code> (Windows) and use the host name instead of the IPv6 address to navigate to the ESM.</p> </div>
	Enable SSH (not available in FIPS mode)	<p>Select this to allow SSH connections. At least one interface must be defined to enable SSH.</p> <div>  <p>ESM and devices use a FIPS capable version of SSH. SSH clients OpenSSH, Putty, dropbear, Cygwin ssh, WinSCP and TeraTerm have been tested and are known to work. If you are using Putty, version 0.62 is compatible and you can download it at http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.</p> </div>
	SSH Port	Enter the specific port that access is allowed through.
	Manage SSH keys	Click SSH Keys . If you have enabled SSH connections, the machine(s) listed communicates. To discontinue communication, delete the machine ID from the list.
	IPv6 Settings	<p>Select Manual or Auto to enable IPv6 mode.</p> <ul style="list-style-type: none"> • If the setting is Off, IPv6 mode is disabled. • If you select Auto, the Primary and Secondary IPv6 fields are disabled. Each host determines its address from the contents of received user advertisements. It makes use of the IEEE EUI-64 standard to define the network ID portion of the address. • If you select Manual, the Primary and Secondary IPv6 fields are enabled. Add the IPv6 addresses in these fields.

Table 3-104 Option definitions (*continued*)

Tab	Option	Definition
Advanced	Set up Internet Control Message Protocol (ICMP) messages and the Intelligent Platform Management Interface (IPMI) on the ESM or its devices.	
	ICMP Messages	Select any of the following options for ICMP: <ul style="list-style-type: none"> • Redirects — The ESM ignores redirect messages. • Dest Unreachable — The ESM generates a message when a packet can't be delivered to its destination for reasons other than congestion. • Enable PING — The ESM sends an <i>Echo Reply</i> message in response to an <i>Echo Request</i> message sent to an IPv6 multicast/anycast address.
	IPMI Settings	If you have an IPMI NIC plugged into a switch and you need to remotely manage the ESM devices through an IPMI card, add the IPMI settings: <ul style="list-style-type: none"> • Enable IPMI Settings — Select to have access to IPMI commands. • VLAN, IP Address, Netmask, Gateway — Enter the settings to configure the network for the IPMI port.
Proxy	If your network uses a proxy server, set up the connection to your ESM.	
	IPv4 or IPv6	On devices, if you have an interface that is using an IPv6 address, you can select IPv6. If not, IPv4 is selected.
	IP Address, Port, Username, Password	Enter the information required to connect to the proxy server.
	Basic Authentication	Select to implement basic authentication checking.
Traffic	Define a maximum data output value for a network and mask to control the rate at which outbound traffic is sent.	
	Table	View the existing controls that you have set up.
	Network column	View the addresses of the networks that the system controls outbound traffic on, based on what you have defined.
	Mask column	(Optional) View the masks for the network addresses.
	Maximum Throughput column	View the maximum throughput you defined for each network.
	Add, Edit, Delete	Manage the network addresses that you want to control.
Static Routes	Static Routes	Add, edit, or remove static routes. A static route is a specified set of instructions regarding how to reach a host or network not available through the default gateway. When you add a static route, the change is pushed to the ESM and immediately takes effect when you click Apply . Upon applying changes, the ESM re-initializes itself, causing all current sessions to be lost.

Set up network traffic control on the ESM

Define a maximum data output value for the ESM.


This feature is helpful when you have bandwidth restrictions and need to control the amount of data that can be sent out by each ESM. The options are kilobits (Kb), megabits (Mb), and gigabits (Gb) per second.



Be careful when configuring this feature because limiting traffic might result in data loss.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Network Settings**, then click the **Traffic** tab.

The table lists the existing controls.

- 3 To add controls for a device, click **Add**, enter the network address and mask, set the rate, then click **OK**.



If you set the mask to zero (0), all the data sent is controlled.

- 4 Click **Apply**.

The outbound traffic speed of the network address you specified is controlled.

Table 3-105 Option definitions

Option	Definition
Network column	Displays the addresses of the networks where the system controls outbound traffic, based on what you have defined.
Mask column	Displays the masks for the network addresses.
Maximum Throughput column	Displays the maximum throughput you defined for each network.
Add, Edit, Delete	Manage the network addresses that you want to control.

Table 3-106 Option definitions

Option	Definition
Network	Type the address of the network where you want to control outbound traffic on.
Mask	Select a mask for the network address. Select 0 for ALL.
Rate	Select kilobits (Kb), megabits (Mb), or gigabits (Gb), then select the rate per second for sending traffic.

See also

[Add throughput rate page on page 171](#)

Add throughput rate page

Define a maximum data output value for a network and mask to control the rate for sending outbound traffic.

Table 3-107 Option definitions

Option	Definition
Network	Type the address of the network where you want to control outbound traffic on.
Mask	Select a mask for the network address. Select 0 for ALL.
Rate	Select kilobits (Kb), megabits (Mb), or gigabits (Gb), then select the rate per second for sending traffic.

See also


[Set up network traffic control on a device on page 32](#)

[Set up network traffic control on the ESM on page 170](#)

Working with host names

The host name of a device is usually more useful than the IP address. You can manage host names so that they are associated with their corresponding IP address.

On the **Hosts** page, you can add, edit, remove, look up, update, and import host names, as well as set the time when an auto-learned host name expires.

When you view event data, you can show the host names associated with the IP addresses in the event by clicking the **Show host names** icon  located at the bottom of view components.

If existing events are not tagged with a host name, the system searches the host table on the ESM and tags the IP addresses with their host names. If the IP addresses are not listed on the host table, the system performs a Domain Name System (DNS) lookup to locate the host names. The search results then show up in the view and are added to the host table.

On the host table, this data is marked as **Auto Learned** and expires after the time designated in the **Entries expire after** field located below the host table on the **System Properties | Hosts** page. If the data has expired, another DNS lookup is performed the next time you select **Show host names** on a view.

The host table lists auto-learned and added host names and their IP addresses. You can add information to the host table manually by entering an IP address and host name individually or by importing a tab-delimited list of IP addresses and host names (see *Import a list of host names*). The more data you enter in this manner, the less time is spent on DNS lookups. If you enter a host name manually, it doesn't expire, but you can edit or remove it.

See also

[Manage host names on page 172](#)

[Import a list of host names on page 173](#)

Manage host names

Perform all the actions necessary to manage host names on the **Hosts** page such as adding, editing, importing, removing, or looking them up. You can also set the expiration time for auto-learned hosts.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Hosts**.
- 2 Select an option and enter the information requested.
- 3 Click **Apply** or **OK**.

Table 3-108 Option definitions

Option	Definition
Add	Add a host name or a host name and its IP address. It's added to the Hosts table.
Edit	Change the host name associated with an IP address.
Remove	Delete the selected item from the table.
Lookup	Look up the host name for an IP address. This is helpful when setting up information for an internal network. When the lookup is complete, the results appear in the table.
Update Hosts	Update the table to reflect any changes made to the list and entries that expired.
Import	Import a tab-delimited list of IP addresses and host names (see <i>Import a list of host names</i>).
Entries expire after	Set the amount of time you want auto-learned host names to remain in the table. If you don't want them to expire, select zero (0) in all fields.

Table 3-109 Option definitions

Option	Definition
Host Name	Type a name for the host. It accepts a string up to 100 characters long.
IP Address	Type the IP address for the host in valid IPv4 or IPv6 notations. You can include a mask.

See also

[Working with host names on page 172](#)

[Import a list of host names on page 173](#)

Import a list of host names

Import a text file that contains IP addresses and the corresponding host names to the host table.

Before you begin

Create the tab-delimited file of IP addresses and host names.

Each record in the file must be listed on a separate line, with the IP address first in IPv4 or IPv6 notation. For example:

102.54.94.97 rhino.acme.com

08c8:e6ff:0100::02ff x.acme.com

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Hosts | Import**.
- 2 Browse to the text file, then click **Upload**. If the file contains IP addresses that are currently on the host table with a different host name, the **Duplicates** page lists the records that are duplicates.
 - To change the host name on the table to the one in the text file, select it in the **Use** column, then click **OK**.
 - To keep the existing host data, don't select the checkbox, then click **OK**.

The new host data is added to the table. The **Auto Learned** column for this data says **No**. Since the data was entered manually, it won't expire.

See also

[Working with host names on page 172](#)

[Manage host names on page 172](#)

Set up DHCP

Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.


When you set up the ESM to deploy in the cloud environment, DHCP is enabled automatically and assigns an IP address. When not in the cloud environment, you can enable and disable DHCP services on the ESM, non-HA Receiver, ACE, and ELM if you have Device Management rights. This would be useful if you need to reset the IP addresses for your network.



Aliases are disabled when DHCP is enabled.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system or a device, then click the **Properties** icon .
- 2 Do one of the following:
 - For the ESM, click **Network Settings**, then click the **Main** tab.
 - For a device, select the device's **Configuration** option, click **Interfaces**, then click the **Network** tab.
- 3 Click **Setup** for the **Interface 1** field, then select **DHCP**.

For devices other than Receivers, you are informed that the changes require an ESM server restart.

- 4 Click **OK**.


Set up DHCP on VLAN

Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

When you set up the ESM to deploy in the cloud environment, DHCP is enabled automatically and assigns an IP address. When not in the cloud environment, you can enable and disable DHCP services on the VLANs, ESM, non-HA Receiver, ACE, and ELM if you have Device Management rights. This would be useful if you need to reset the IP addresses for your network.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system or a device, then click the **Properties** icon .
- 2 Do one of the following:
 - For the ESM, click **Network Settings**, then click the **Main** tab.
 - For a device, select the device's **Configuration** option, click **Interfaces**, then click the **Network** tab.
- 3 Click **Setup** for the **Interface 1** field, then click **Advanced**.
- 4 Click **Add VLAN**, type the **VLAN**, then select **DHCP**.
- 5 Click **OK** to return to the **Network Settings** page, then click **Apply**.

For devices other than Receivers, you are informed that the changes require an ESM server restart.

System time synchronization

Since activities generated by the ESM and its devices are time stamped, it is important that the ESM and devices be synchronized to keep a constant frame of reference for data they gather. You can set the ESM system time or select to have the ESM and devices synchronized to an NTP server.

See also

[Set up system time on page 175](#)

[Sync device clocks on page 176](#)

Set up system time

Before you begin

If you want to add NTP servers to the ESM, set up the NTP servers and have their authorization keys and key IDs.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties** and ensure **System Information** is selected.
- 2 Click **System Clock (GMT)**, define the settings, then click **OK**.




NTP server addresses on ADM or DBM devices must be IP addresses.

The server information is saved in the configuration file. You can then access the list of NTP servers again and check their status.

Table 3-110 Option definitions

Option	Definition
Set the ESM System Time (GMT) to	If you aren't using an NTP server to synchronize the system's time, make sure that this date and time is set to GMT.
Use NTP Server(s) for time synchronization	Select this option to use NTP servers to synchronize the system's time instead of using the system clock.

Table 3-110 Option definitions *(continued)*

Option	Definition
NTP Server column	Add the IP addresses for NTP servers by clicking in this column. You can add up to 10 servers.  NTP server addresses on ADM or DBM devices must be IP addresses.
Authentication key and Key ID columns	Type the authentication key and key ID for each NTP server (contact your network administrator if you do not know them).
Status	Click to view the status of the NTP servers on the list. If you made changes to the list of servers, you must click OK to save the changes and close the page, then open the page again prior to clicking Status .

See also

[System time synchronization on page 175](#)

Sync device clocks

You can sync the device clocks with the ESM clock so that the data generated by the various systems reflects the same time setting.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties** or device **Properties**, then click **Sync** in the **Sync Device Clock** field.

You are informed when the sync is complete or if there is a problem.

- 2 Click **Refresh** to update the data on the **System Information** or device **Information** page.

See also

[System time synchronization on page 175](#)

Install a new certificate

The ESM ships with a default self-signed security certificate for esm.mcafee.local. Most web browsers display a warning that the certificate's authenticity can't be verified. Once you obtain the SSL key certificate pair that you want to use for your ESM, you must install it.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **ESM Management**.
- 2 On the **Key Management** tab, click **Certificate**.
- 3 Make the selections, then click **Close**.

Option	Definition
Upload Certificate	Install certificate, key, and optional chain files, if you have them. You are asked to upload the .crt file, then the .key file, and finally the chain files.
Self-Signed Certificate	Generate and install a self-signed security certificate for the ESM. Click Generate , then enter the information in the Manage Certificate page. Click OK , then click Generate .

Option	Definition
Signed Certificate Request	Generate a certificate request to send to a certificate authority for signature. <ul style="list-style-type: none"> Click Generate, enter the information in the Manage Certificate page, then click OK. Download the .zip file that holds a .crt and a .key file. Extract the .crt file, then send it to the certificate authority.
Regenerate default McAfee certificates	Regenerate the original certificate.

Configure profiles

Define profiles for syslog-based traffic so you can perform setups that share common information without entering the details each time. You can also add a remote command profile (URL or Script) and use it on a view or an alarm.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Profile Management**.
- 2 To add a profile, click **Add** on the **System Profiles** tab, then fill in the profile data.
- 3 To add a remote command, click the **Remote Command** tab, then fill in the requested information.
- 4 Click **OK**.

Table 3-111 Option definitions

Option	Definition
System Profiles table	View the profiles currently on the system.
Add	Add a profile.
Edit	Change the selected profile.
Remove	Delete the selected profile.

Table 3-112 Option definitions

Option	Definition
Authentication Password	If you select authNoPriv or authPriv in the Security Level field, this field is active. Enter the password for the authentication protocol selected in the Authentication Protocol field.
Authentication Protocol	If you select authNoPriv or authPriv in the Security Level field, this field is active. Select the type of protocol for this source: MD5 or SHA1 . SHA1 and SHA see the same protocol type.
Community Name	Type the SNMP trap's community string.
Compression	For Remote Share SCP, select if you want to use compression.
Encryption	For Remote Share FTP, select if you want to use encryption.
Engine ID	Enter the SNMPv3 engine ID of the trap sender. Not a required field.
Event Logs	The default WMI event logs are SYSTEM, APPLICATION, and SECURITY, but other logs are supported. When entering additional names, remember that they are case sensitive, separated by a comma, and should not have spaces between them. You must have access to read logs. You can only pull security logs if you are an administrator. You can pull WMI data source logs without administrator rights if they are set up correctly.

Table 3-112 Option definitions *(continued)*

Option	Definition
Facility	Select the facility the event forwarding message is sent to.
Interval	Select the interval, in minutes, that the Receiver is to check the WMI provider for new events.
IP Address	SNMP Trap: Type the IP address of the eEye server that is sending trap information. Event Forwarding: Type the IP address the events are forwarded to.
Password	The password used to connect to the WMI provider.
Privacy Protocol	If you select authPriv in the SNMP Security Level field, this field is active. Select either DES or AES . In FIPS mode, AES is the only option available.
Profile Agent	Select the agent for this profile. The remaining fields vary based on your selection in this field.
Profile Name	Type a descriptive name for this profile.
Profile Type	Select the type of profile. The remaining fields on this page vary based on your selection in this field. Most of them are self-explanatory.
Port	Change the connection port if the default is not correct.
Protocol	Select the transport protocol.
Remote IP Address, Remote Mount Point, Remote Path	If you selected CIFS or NFS as the profile agent, type this information for the storage device.
Security Level	Select the security level for this SNMPv3 profile. <ul style="list-style-type: none"> • noAuthNoPriv — No authentication protocol and no privacy protocol • authNotPriv — Authentication protocol but no privacy protocol • authPriv — Both authentication and privacy protocol The Authentication and Privacy fields become active based on the security level you select.
Send Packet	Select if you want to send the event packet.
Severity	Select the severity of the information being forwarded.
Username	The user name used to connect to the WMI provides. For domain users, enter user name as domain\user.


Table 3-113 Option definitions

Option	Definition
Remote Commands table	View the remote commands currently on the system.
Add	Add a new remote command.
Edit	Change the selected remote command.
Remove	Delete the selected remote command.

Table 3-114 Option definitions

Option	Definition
Name	Type a name for this remote command profile.
Description	Describe what this command does.
Type	Select the type of remote command this is.
Time Zone	Select the time zone to use.

Table 3-114 Option definitions *(continued)*

Option	Definition
Date Format	Select the format for the date.
Host, Port, Username, Password	Type the information for the SSH connection.
Command String	Type the command string for the SSH connection. To insert variables into the command string, click the Insert variable icon  and select the variables.

SNMP configuration

Configure the settings used by the ESM to send link up and down and cold and warm start traps, both from the ESM and each device. Retrieve Management Information Base (MIB)-II system and interface tables, and allow discovery of the ESM through an SNMP walk.

SNMPv3 is supported with NoAuthNoPriv, AuthNoPriv, and AuthPriv options, using MD5 or Secure Hash Algorithm (SHA) for authentication and Data Encryption Standard (DES) or Advanced Encryption Standard (AES) for encryption. MD5 and DES are not available in FIPS compliance mode.

SNMP requests can be made to an ESM for ESM and Receiver, health information. SNMPv3 traps can be sent to an ESM to add to the blacklist of one or more of its managed devices. All McAfee appliances can also be configured to send link traps and boot traps to destinations of your choosing (see *SNMP and the McAfee MIB*).

See also

[Configure SNMP settings on page 179](#)

[Set up SNMP trap for power failure notification on page 181](#)

[SNMP and the McAfee MIB on page 182](#)

[Pull the MIB from the ESM on page 185](#)

Configure SNMP settings


Define the settings used by the ESM for inbound and outbound SNMP traffic. SNMP queries can only be performed by users whose user names don't include a space.



Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **SNMP Configuration**.
- 2 Enter the required information on the **SNMP Requests** and **SNMP Traps** tabs.
- 3 Click **OK**.

Table 3-115 Option definitions

Tab	Option	Definition
SNMP Requests	Request Port	Select the port where the traffic passes.
	Accept	Select the types of traps to accept.
	Allow SNMPv1/2c	Select to allow SNMP version 1 and version 2 traffic, and type the community type.
	Allow SNMPv3	Select to allow SNMP version 3 traffic, and select the security level, authentication protocol, and privacy protocol.
	Trusted IP Addresses	View the IP addresses that the ESM considers trusted or allows. You can add new addresses and edit or remove existing ones. The IP address can include a mask.
	View Device IDs	View a list of device IDs you can use when sending SNMP requests.
	View MIB	View the McAfee MIB, which defines the object identifiers (OIDs) for each object or characteristic of interest.
SNMP Traps	Trap Port	On the SNMP Traps tab, set the port where the cold/warm trap traffic as well as the blacklist entry and link up/link down traffic passes.
	Link Up/Down Traps	Select if you want Link Up and Link Down traps to be sent. If you select this feature and you are using multiple interfaces, you are notified when an interface goes down as well as when it comes back up. <div data-bbox="727 1163 1520 1346">  Cold/warm trap traffic is automatically allowed. A cold start trap is generated any time the SNMP service is restarted. The SNMP service restarts after SNMP configuration changes, a user is modified, a group is modified, a user logs in with remote authentication, the ESM reboots, cpservice restarts, and other situations. A warm start trap is generated when you reboot the system. </div>
	Database Up/Down Traps	Select if you want an SNMP trap sent when the database (cpservice, IPSDBServer) goes up or down.
	Security Log Failure Trap	Select if you want an SNMP trap sent when a log is not written to the log table.
	General Hardware Failure	Select to be notified if either of the ESM power supplies fail (general hardware or DAS). This helps avoid a system shutdown due to power failure.
	Destinations	Select the profile names of the systems you want the notifications sent to. The table shows all available SNMP trap profiles on the system. To edit this list, click Edit Profiles and add, edit, or remove profiles from the Profile Manager list.
Tab	Option	Definition
SNMP Requests	Request Port	Select the port where the traffic passes.
	Accept	Select for device health requests to be accepted.

Tab	Option	Definition
	Allow SNMPv1	Select to allow SNMP version 1 and version 2 traffic, and set the community string.
	Allow SNMPv3	Select to allow SNMP version 3 traffic, and select the security level, authentication protocol, and privacy protocol.
	Trusted IP Addresses	View the IP addresses that the device allows or considers trusted. You can add new addresses and edit or remove existing ones. The IP address can include a mask.  A trusted IP address must be present.
	View MIB	View the McAfee MIB, which defines the object identifiers (OIDs) for each object or characteristic of interest.
SNMP Traps	Trap Port	Set the port where the cold/warm trap traffic, blacklist entry, and link up/link down traffic passes.
	Link Up/Down Traps	Select to send Link Up and Link Down traps. If you select this feature and are using multiple interfaces, you are notified when an interface goes down and when it comes back up.  Cold/warm trap traffic is automatically allowed. A cold start trap is generated when there is a hard shut-down or hard reset. A warm start trap is generated when you reboot the system.
	Database Up/Down Traps	Select to send an SNMP trap when the database (cpservice, IPSDBServer) goes up or down.
	Security Log Failure Trap	Select to send an SNMP trap when a log is not written to the log table.
	Destinations	Select the profile names of the systems where you want the notifications sent. The table shows all available SNMP trap profiles on the system. To edit this list, click Edit Profiles and add, edit, or remove profiles from the Profile Manager list.

See also[SNMP configuration on page 179](#)[Set up SNMP trap for power failure notification on page 181](#)[SNMP and the McAfee MIB on page 182](#)[Pull the MIB from the ESM on page 185](#)**Set up SNMP trap for power failure notification**


Select an SNMP trap to notify you about hardware and DAS power failures, to keep the system from shutting down due to a power failure.

Before you begin

- Verify that you have administrator rights or belong to an access group with alarm management privileges.
- Prepare the SNMP trap Receiver (required if you don't already have an SNMP trap Receiver).

For details about product features, usage, and best practices, click **?** or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **SNMP Configuration**, then click the **SNMP Traps** tab.
- 3 In **Trap Port**, type 162, then select **General Hardware Failure**, and click **Edit Profiles**.
- 4 Click **Add**, then enter the requested information like this:
 - **Profile Type** — Select **SNMP Trap**.
 - **IP Address** — Type the address where you want to send the trap.
 - **Port** — Type 162.
 - **Community Name** — Type `Public`.



Remember what you type in the **Port** and **Community Name** fields.

- 5 Click **OK**, then click **Close** on the **Profile Manager** page.

The profile is added to the **Destinations** table.

- 6 Select the profile in the **Use** column, then click **OK**.

When a power supply fails, an SNMP trap is sent and a health status flag appears next to the device on the system navigation tree.

See also

[SNMP configuration on page 179](#)

[Configure SNMP settings on page 179](#)

[SNMP and the McAfee MIB on page 182](#)

[Pull the MIB from the ESM on page 185](#)

SNMP and the McAfee MIB

Several aspects of the McAfee product line can be accessed through SNMP. The McAfee MIB defines the object identifiers (OIDs) for each object or characteristic of interest.

The MIB defines object groups for:

- **Alerts** — An ESM can generate and send alert traps using Event Forwarding. A Receiver can receive alert traps by configuring a McAfee SNMP data source.
- **Flows** — A Receiver can receive flow traps by configuring a McAfee SNMP data source.
- **ESM Health Requests** — An ESM can receive and respond to health requests for itself and the devices it manages.
- **Blacklist** — An ESM can receive traps defining entries for blacklists and quarantine lists, which it then applies to the devices that it manages.

The McAfee MIB also defines textual conventions (enumerated types) for values including:

- The action performed when an alert was received
- Flow direction and state
- Data source types
- Blacklist actions

The McAfee MIB is syntactically compliant with SNMPv2 Structure of Management Information (SMI). McAfee products that use SNMP can be configured to work over SNMPv1, SNMPv2c, and SNMPv3, including authentication and access control.

Health requests are made by using the SNMP `GET` operation. The SNMP `GET` operation is used by SNMP manager applications to retrieve values from the managed objects maintained by the SNMP agent (in this case, the ESM). The applications typically perform an SNMP `GET` request by providing the host name of the ESM and OIDs, with the specific instance of the OID.

The ESM responds by populating the OID bindings with the results of the health request.

The following tables show the meaning of the ESM and Receiver OIDs.


Table 3-116 ESM health

Request and response OID	Units	Response value	Meaning
1.3.6.1.4.1.23128.1.3.1.1	Percent	4	Percentage combined instantaneous CPU load
1.3.6.1.4.1.23128.1.3.1.2	MB	3518	Total RAM
1.3.6.1.4.1.23128.1.3.1.3	MB	25	Available RAM
1.3.6.1.4.1.23128.1.3.1.4	MB	1468006	Total HDD space partitioned for ESM database
1.3.6.1.4.1.23128.1.3.1.5	MB	1363148	Free HDD space available for ESM database
1.3.6.1.4.1.23128.1.3.1.6	seconds since 1970-1-1 00:00:0.0 (GMT)	1283888714	Current system time on the ESM
1.3.6.1.4.1.23128.1.3.1.7		8.4.2	ESM version and buildstamp
1.3.6.1.4.1.23128.1.3.1.8		4EEE:6669	Machine ID of the ESM
1.3.6.1.4.1.23128.1.3.1.9		ESM	ESM model number

Table 3-117 Receiver health

Request and response OID	Units	Response value	Meaning
1.3.6.1.4.1.23128.1.3.3.1.x		Receiver	Receiver name
1.3.6.1.4.1.23128.1.3.3.2 .x		2689599744	ESM unique identifier of the Receiver
1.3.6.1.4.1.23128.1.3.3.3.x		1	Indicates that communication with the Receiver is available (1) or not available (0)
1.3.6.1.4.1.23128.1.3.3.4.x		Ok	Indicates the status of the Receiver
1.3.6.1.4.1.23128.1.3.3.5.x	percent	2	Percentage combined instantaneous CPU load
1.3.6.1.4.1.23128.1.3.3.6.x	MB	7155	Total RAM
1.3.6.1.4.1.23128.1.3.3.7.x	MB	5619	Available RAM
1.3.6.1.4.1.23128.1.3.3.8.x	MB	498688	Total HDD space partitioned for Receiver database

Table 3-117 Receiver health *(continued)*

Request and response OID	Units	Response value	Meaning
1.3.6.1.4.1.23128.1.3.3.9.x	MB	472064	Free HDD space available for Receiver database
1.3.6.1.4.1.23128.1.3.3.10.x	seconds since 1970-1-1 00:00:0.0 (GMT)	1283889234	Current system time on the Receiver
1.3.6.1.4.1.23128.1.3.3.11.x		7.1.3 20070518091421a	Receiver version and buildstamp
1.3.6.1.4.1.23128.1.3.3.12.x		5EEE:CCC6	Machine ID of the Receiver
1.3.6.1.4.1.23128.1.3.3.13.x		Receiver	Receiver model number
1.3.6.1.4.1.23128.1.3.3.14.x	alerts per minute	1	Alert rate (per minute) for last 10 minutes
1.3.6.1.4.1.23128.1.3.3.15.x	flows per minute	2	Flow rate (per minute) for last 10 minutes
 x = Device ID. To access a list of device IDs, go to System Properties SNMP Configuration , then click View Device IDs .			

Events, flows, and blacklist entries are sent using SNMP traps or inform requests. An alert trap sent from an ESM configured to do Event Forwarding might look something like this:

OID	Value	Meaning
1.3.6.1.4.1.23128.1.1.1	780	ESM alert ID
1.3.6.1.4.1.23128.1.1.2	6136598	Device alert ID
1.3.6.1.4.1.23128.1.1.4	2	Device ID
1.3.6.1.4.1.23128.1.1.5	10.0.0.69	Source IP address
1.3.6.1.4.1.23128.1.1.6	27078	Source Port
1.3.6.1.4.1.23128.1.1.7	AB:CD:EF:01:23:45	Source MAC
1.3.6.1.4.1.23128.1.1.8	10.0.0.68	Destination IP address
1.3.6.1.4.1.23128.1.1.9	37258	Destination Port
1.3.6.1.4.1.23128.1.1.10	01:23:45:AB:CD:EF	Destination MAC
1.3.6.1.4.1.23128.1.1.11	17	Protocol
1.3.6.1.4.1.23128.1.1.12	0	VLAN
1.3.6.1.4.1.23128.1.1.13	1	Flow direction
1.3.6.1.4.1.23128.1.1.14	20	Event count
1.3.6.1.4.1.23128.1.1.15	1201791100	First time
1.3.6.1.4.1.23128.1.1.16	1201794638	Last time
1.3.6.1.4.1.23128.1.1.17	288448	Last time (microseconds)
1.3.6.1.4.1.23128.1.1.18	2000002	Signature ID

OID	Value	Meaning
1.3.6.1.4.1.23128.1.1.19	ANOMALY Inbound High to High	Signature description
1.3.6.1.4.1.23128.1.1.20	5	Action taken
1.3.6.1.4.1.23128.1.1.21	1	Severity
1.3.6.1.4.1.23128.1.1.22	201	Data source type or result
1.3.6.1.4.1.23128.1.1.23	0	Normalized signature ID
1.3.6.1.4.1.23128.1.1.24	0:0:0:0:0:0:0	IPv6 source IP address
1.3.6.1.4.1.23128.1.1.25	0:0:0:0:0:0:0	IPv6 destination IP address
1.3.6.1.4.1.23128.1.1.26		Application
1.3.6.1.4.1.23128.1.1.27		Domain
1.3.6.1.4.1.23128.1.1.28		Host
1.3.6.1.4.1.23128.1.1.29		User (source)
1.3.6.1.4.1.23128.1.1.30		User (destination)
1.3.6.1.4.1.23128.1.1.31		Command
1.3.6.1.4.1.23128.1.1.32		Object
1.3.6.1.4.1.23128.1.1.33		Sequence Number
1.3.6.1.4.1.23128.1.1.34		Indicates whether generated in a trusted or untrusted environment
1.3.6.1.4.1.23128.1.1.35		ID of session that generated the alert

The numbers mean:

- 1.3.6.1.4.1.23128 — The McAfee IANA-assigned enterprise number
- The final number (1–35) — For reporting the various characteristics of the alert

For the full details of McAfee MIB definition, see <https://x.x.x.x/BrowseReference/NITROSECURITY-BASE-MIB.txt>, where x.x.x.x is the IP address of your ESM.

See also

[SNMP configuration on page 179](#)

[Configure SNMP settings on page 179](#)

[Set up SNMP trap for power failure notification on page 181](#)

[Pull the MIB from the ESM on page 185](#)

Pull the MIB from the ESM


View the objects and notifications for interfacing with the ESM.

The objects and notifications defined in this MIB are used to send requests:

- To an ESM requesting health status information for the ESM itself or for Receiver devices
- To a device to request its health status information.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **SNMP Configuration**, then click **View MIB**.

A list of base MIB definitions opens.

See also

[SNMP configuration on page 179](#)

[Configure SNMP settings on page 179](#)

[Set up SNMP trap for power failure notification on page 181](#)

[SNMP and the McAfee MIB on page 182](#)

Managing the database

Manage the ESM database to provide information and settings as you set up features on your system.

You can do the following:

- Manage database index settings.
- Configure the data retention policy and space allocation for events and flows.
- View and print information about the database memory utilization of events.

If you have more than four CPUs on a VM, you can use the additional storage space for system storage, data storage, and high-performance storage.



If you remove more than one drive from the ESM VM at one time, all previous ELM searches can be lost. To avoid loss, export the ELM search results before removing the drives.

Set up database archival

ESM divides data into partitions. When a partition reaches its maximum size, it becomes inactive and is deleted. You can configure a storage location for inactive partitions so they aren't deleted.



To prevent potential data loss when archiving on a redundant ESM, we recommend that you set up archival prior to setting up ESM redundancy. When setting this up on a redundant ESM, do not use the same archival path that the primary uses.





Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Database | Archival**.
- 2 Fill in the fields, which vary depending on the type you select.
- 3 Click **OK** to save the settings.

As partitions become inactive, they are copied to this location.

Table 3-118 Option definitions

Option	Definition
Enabled	Select to activate inactive partition archiving.
Type	<p>Select the type of storage. Your options are CIFS, NFS, iSCSI, and, if you have a SAN card installed, SAN.</p> <p> Using a CIFS share type with Samba server versions later than 3.2 can result in data loss.</p>
Size	Select the maximum amount of storage space you want to allocate on this device.
SAN volume	If you selected the SAN type, select the SAN volume. All volumes that are ready to store data is listed.
Edit	You can format other volumes and add them to the SAN volume list.
Remote IP Address, Remote Mount Point, Remote Path	<p>If you selected CIFS or NFS, type the information for the storage device in each of these fields.</p> <p> When setting up archiving for redundant ESMs, ensure that the remote path differs from the archiving settings on the primary ESM.</p>
User name, Password	<p>If you selected CIFS, you must enter the user name and password for the storage device.</p> <p> When connecting to a CIFS share, do not use commas in your password.</p>
iSCSI Device and iSCSI IQN	<p>Select the iSCSI storage device and the iSCSI Qualified Name (IQN).</p> <p> Trying to attach multiple devices to one IQN can cause data loss and other configuration problems.</p> <p>If you set up the ELM connection with the iSCSI SAN and have an all-in-one ESM/ Receiver/ELM device, the fields list the device and its iSCSI Qualified Names (IQNs). If you have dedicated ESM and ELM devices, configure the connection to the iSCSI device.</p>
Connect	Click to test the connection.
Data allocation	Adjust the total number of event, flow, and log records that can be saved on this device in the Events , Flows , and Logs fields.
Event Partitions, Flow Partitions, or Log Partitions tab	You can reactivate up to 100 partitions by selecting them in the Active column.

Set up ESM data storage

If you have an Internet Small Computer System Interface (iSCSI), Storage Area Network (SAN), or Direct-attached storage (DAS) device connected to the ESM, you can set them up for data storage.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Database** | **Archival**.
- 2 Click the data storage device tabs, select an action, then fill in the requested information.
The available tabs depend on the storage types connected to the ESM.
- 3 Click **Cancel** to close the page.

Table 3-119 Option definitions

Option	Definition
Name	Type the name of the iSCSI device.
IP Address	Type the IP address for the iSCSI device
Port	Select the port for the iSCSI device.

Set up ESM VM data storage

If your ESM VM has more than four CPUs, the **VM Data** option is available on the **Database** page, allowing you to use the additional storage you have available for the VM's system storage, data storage, and high performance storage.

Each drop-down list on the **Data Allocation** page includes the available storage drives that are mounted on the VM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Database** | **VM Data**.
- 2 In each field, select the drive you want the data stored on. Each drive can only be selected once.
- 3 Click **OK**.

Increase number of available accumulator indexes

Due to the number of enabled standard indexes on the ESM, you can only add five indexes to an accumulator field. If you need more than five, you can disable standard indexes that you are not currently using, such as sessionid, src/dst mac, src/dst port, src/dst zone, src/dst geolocation, up to a maximum of 42.

Task

For details about product features, usage, and best practices, click ? or **Help**.



The ESM uses standard indexes when generating queries, reports, alarms, and views. If you disable any of them, then try to generate a query, report, alarm, or view that uses them, you are notified that it can't be processed because an index is disabled. You are not told which index is affecting the process. Due to this limitation, do not disable standard indexes unless you determine it is absolutely necessary.

- 1 On the system navigation tree, select **System Properties**, then click **Database**.
- 2 Click **Settings**, then click the **Accumulator Indexing** tab.

- From the drop-down list, click **Standard Indexes**, then select **Show standard indexes**.

The standard indexes are listed in the **Enabled** area.

- Click the standard indexes to be disabled, then click the arrow to move them to the **Available** area.

The number in the **remaining** statement in the top right corner of the page increases with each standard index that you disable.

You can now enable more than five accumulator indexes for the accumulator field that you select (see *Manage accumulator indexing*).

Set up data retention limits

If you have a configuration that is sending historical data to the system, you can select the length of time that you want events and flows maintained as well as limit the amount of historical data inserted.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- On the system navigation tree, select **System Properties**, then click **Database | Data Retention**.
- Select how long you want events and flows retained and if you want to restrict historical data.
- Click **OK**.

Table 3-120 Option definitions

Option	Definition
Keep all data allowed	Select to maintain the maximum number of events or flows that the system allows.
Keep data for the last	Select if you only want to maintain events and flows for the length of time you specify.
Restrict insertion of	Select if you want to restrict historical data, and select how old the data can be in the Don't insert data older than field.

Define data allocation limits


The maximum number of event and flow records that are maintained by the system is a fixed value. Data allocation allows you to set how much space to allocate for each, and how many records are searched to optimize querying.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- On the system navigation tree, select **System Properties**, then click **Database | Data Allocation**.
- Click the markers on the number lines and drag them to the desired numbers, or click the arrows in the **Events** and **Flows** fields.
- Click **OK**.

Table 3-121 Option definitions

Option	Definition
Top slider	Indicate how much of the total space must be allocated for events and how much for flows.
Bottom slider	Set how many event and flow records are searched when a query is performed.
 This slider doesn't appear if there isn't an SSD device.	

Manage database index settings

Configure options for indexing specific fields of data in the database. If data is not indexed, it's stored but is not displayed in most query results.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Database | Settings**.
- 2 To change the current settings in the **Events** and **Flows** columns, click the item you want to change and select a new setting from the drop-down list.
- 3 If you select **Custom** in the **Port** columns, the **Port Values** screen opens so you can select or add a new port value.
- 4 Click **OK**.

Table 3-122 Option definitions

Option	Definition
Table	View the indexing settings for the ESM and its devices.
Mac Address columns	Select the current setting and select one of the options. If the setting for a device is Inherit , it uses the system settings.
Port columns	Click on the current setting and select one of the options. If you select Custom , the Port Values page opens so you can select or add a port value.

Table 3-123 Option definitions

Option	Definition
Add Value	Add the selected value to the Current Value field.
New	Add a new port value by typing a name and its value. It's added to the list and can be used in the future.
Edit	Change the name or value for a custom port.
Delete	Delete a custom port from the list of ports.
Current Value	Enter a port value by typing it in or highlighting it and clicking Add Value .

Manage accumulator indexing

If you have custom fields that pull numeric data from a source, accumulator indexing can perform sums or averages over time on this data. You can accumulate several events together and average their value or generate a trending value.

Before you begin

Set up an accumulator indexing custom type (see *Create custom types*).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Database**.
- 2 Click **Settings**, then click the **Accumulator Indexing** tab.
- 3 Select the indexes, then click **OK**.

You can now set up an accumulator query to display the results.

Table 3-124 Option definitions

Option	Definition
Drop-down list	Select the accumulator field you want to add indexes to. If you need more than five indexes, select Standard Indexes .
Show standard indexes	Select this option to view the standard indexes in the Enabled and Available lists.
Available list	If you selected an accumulator field, select the indexes to enable, then click the arrow to move them to the Enabled list. The remaining statement in the top right corner of the page will let you know how many more indexes you can select for this field.
Enabled list	View the enabled indexes. If you selected Show standard indexes , the standard indexes will be listed. To remove one, select it, then click the arrow to move it back to the Available list. If you remove a standard index, the number of accumulator indexes you can add to the accumulator field will increase.
From this point forward	Select if you want to use these indexes on data generated from this point forward
Rebuild past data	Select if you want to use these indexes on past data, then select the date you want to start with. If you choose to do this, the partitions containing the data need to be rebuilt.

View database memory utilization

View and print tables that detail how database memory is being used.

Task

For details about product features, usage, and best practices, click **?** or **Help**.



- 1 On the system navigation tree, select **System Properties**, then click **Database | Memory Use**.
The **Events** and **Flows** tables list the memory utilization of the database.
- 2 To print the reports, click the **Print** icon .

Table 3-125 Option definitions

Option	Definition
Events table	View memory usage for events by index name.
Flows table	View memory usage for flows by index name.
	Print a memory utilization report.

Working with users and groups

Users and groups must be added to the system so that they have access to the ESM, its devices, its policies, and their associated privileges.

When in FIPS mode, ESM has four possible user roles: **User**, **Power User**, **Key & Certificate Admin**, and **Audit Admin**. When not in FIPS mode, there are two types of user accounts: **System Administrator** and **General User**.

The **Users and Groups** page has two sections:

- **Users** — Names of users, the number of sessions that each user has open currently, and the groups to which they belong.
- **Groups** — Names of groups and a description of the privileges assigned to each one.



You can sort the tables by clicking **Username**, **Sessions**, or **Group Name**.

Group privileges

When you set up a group, you set the privileges for the members of the group.

If you select **Limit access of this group** on the **Privileges** page of **Add Group (System Properties | Add Group)**, access to these features is limited.

- **Actions toolbar** — Users can't access device management, multi-device management, or Event Streaming Viewer.
- **Alarms** — The users in the group have no access to alarm management recipients, files, or templates. They can't create, edit, remove, enable, or disable alarms.
- **Asset Manager and Policy Editor** — Users can't access these features.
- **Case Management** — Users can access all features except **Organization**.
- **ELM** — Users can perform enhanced ELM searches but can't save them or access ELM device properties.
- **Filters** — Users can't access **String Normalization**, **Active Directory**, **Assets**, **Asset Groups**, or **Tags** filter tabs.
- **Reports** — Users can only run a report that emails the output to them.
- **System Properties** — Users can access only **Reports** and **Watchlists**.
- **Watchlists** — Users can't add a dynamic watchlist.
- **Zones** — Users can view only zones they have access to in their list of zones.

Add a user

If you have **User Administration** privileges, you can add users to the system so that they have access to the ESM, its devices, policies, and associated privileges. Once added, user settings can be edited or removed.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties | Users and Groups**.
- 2 Enter your password, then click **OK**.
- 3 In the **Users** section, click **Add**, then fill in the information requested.
- 4 Click **OK**, then type your password again.


Users are added to the system with the privileges assigned to the groups they belong to. User names appear in the **Users** section of the **Users and Groups** page. Next to each user name, an icon indicates whether the account is enabled. If the user has administrator privileges, a different icon  appears next to their name.


Table 3-126 Option definitions

Option	Definition
Username	Enter a user name. If you are using CAC settings, the user name is the user's 10-digit EDI-PI.
User Alias	(Optional) Enter an alias if you do not want the user's name to be visible. If you are using CAC settings, this can be the user's name.
Password	Click Set Password , enter a unique password for the account and confirm it, then click OK .

Table 3-126 Option definitions (continued)

Option	Definition
Role (FIPS mode only)	<p>Select a role for this user. The options are:</p> <ul style="list-style-type: none"> • User — These users can't be added to a group containing Power User privileges. • Power User — These users are considered system administrators for all Unified Capabilities Approved Products List (UCAPL) purposes, but they might not have all the privileges of a system administrator. This role is required for a user to be assigned to a group containing any of these privileges: <ul style="list-style-type: none"> • System Management • User Administration • Policy Administration • Add/Delete Policies • Custom Rules and Variables • Global Blacklisting • Key & Certificate Admin — This role is required to perform any key management functions. A user with this role can't be added to a group containing Power User privileges. • Audit Admin — This role is required to configure the logs. A user with this role can't be added to a group containing Power User privileges.
Administrator Rights (not in FIPS mode)	Select if you want the user to have administrator privileges. The system administrator can grant privileges to general users by creating access groups and assigning users to these groups. The system administrator is the only user who has access to all areas of the system, including the users and groups area.
Disable account	Select if you want to block the user from accessing their account on the ESM (see <i>Disable or re-enable a user account</i>).
Email Address	<p>Add the user's email address, which is optional unless the user receives report or alarm notifications.</p> <ul style="list-style-type: none"> • If the email address is already on the system, select it from the Email Address drop-down list. • If the address is not in the system, click Email Address and add the address to the system.
Mobile SMS	<p>Add the user's SMS (text) address.</p> <ul style="list-style-type: none"> • If the SMS number is already in the system, select it from the Mobile SMS drop-down list. • If the address is not in the system, click Mobile SMS and add the address to the system.
User is a member of	Select the groups where this user should be a member.

Table 3-127 Option definitions

Option	Definition
Users table	Lists the users with access to the ESM.
Groups table	Lists the groups that are set up on the ESM.
Add, Edit, and Remove	<ul style="list-style-type: none"> • To the right of the Users table, add new users or edit or remove existing users. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin: 5px 0;">  Before removing a user, ensure that the user isn't set as the assignee in an alarm. </div> <ul style="list-style-type: none"> • To the right of the Groups table, add new groups, and assign users and rights to them.

Select user settings

The **User Settings** page gives you the option to change several default settings. You can change the time zone, date format, password, default display, and console language. You can also choose whether to show disabled data sources, the **Alarms** tab, and the **Cases** tab.



Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation bar of the ESM console, click **options**.
- 2 Verify that **User Settings** is selected.
- 3 Change the settings as needed, then click **OK**.

The console changes its appearance based on your settings.

Table 3-128 Option definitions

Option	Definition
Select a time zone and date format	<p>Change the time zone on the first drop-down list or the data format on second one.</p> <div>  <p>All views, queries, and settings show event, flow, and log data relative to this time zone and in this date format unless explicitly noted otherwise. If you change this time zone, incorrect data could be generated. Therefore, we recommend that it always be set to GMT.</p> </div>
Change Password	On the Change Username and Password page, change the user name and password you use to access the ESM console. If you do not want your name showing up on the console navigation bar, enter a different user name in the Alias field.
Default Display	Select the system navigation tree display type that you want to appear by default when the system opens.
Language	Select the language for the console.
Show disabled data sources in the system tree	Select this option if you want disabled data sources to show up in the system navigation tree. They will be indicated by this icon  .
Show Alarms Pane	Select this option if you want the Alarms pane to appear on the console.
Show Case Management Pane	Select this option if you want the Cases pane to appear on the console.

Setting up security

Use login security to set up standard login settings, configure the access control list (ACL), and define Common Access Card (CAC) settings. You can also enable Remote Authentication Dial In User Service (RADIUS), Active Directory, and Lightweight Directory Access Protocol (LDAP) authentication (only available if you have system administrator privileges).

Key features

The McAfee family of solutions is hard to find on a network and even harder to attack. Devices have no IP stack by default, so packets can't be addressed directly.

Communication with a device is achieved through the McAfee Secure Encrypted Management (SEM) technology. SEM is an in-band Advanced Encryption Standard (AES) encrypted channel that mitigates the risk of playback or man-in-the-middle types of attacks.



A device communicates only when addressed by an authorized ESM via the SEM channel. It does not initiate communications on its own. Communication between an ESM and the ESM console is also sent over an encrypted connection, which is FIPS-compliant.

The ESM retrieves authenticated and encrypted signature and software updates from the McAfee central server from an encrypted communication mechanism. Mechanisms, both hardware- and software-based, are in place to make sure devices are managed only from a properly authorized ESM.

Define standard login settings


Adjust the settings for standard login procedures by defining how many login attempts can be made in a specified period of time, how long the system can be inactive, password settings, and whether to show the last user ID upon login.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the system navigation tree, select **System Properties**, then click **Login Security**.
- 2 Set the options on the **Standard** tab.
- 3 Click **OK** or **Apply**.

Table 3-129 Option definitions

Option	Definition
Allowed failed login attempts	Specify the number of consecutive unsuccessful logins that are allowed in a single session. If this number is exceeded in the amount of time specified, the account will be locked and the system administrator must unlock it using Users and Groups . A value of 0 means that infinite login attempts are allowed.  The master account can't be locked.
Failed login attempts timeframe	Define the time frame for successive failed login attempts. The range is 0 to 1440 minutes. This field works in conjunction with Allowed Failed Login Attempts . When the number of allowed failed attempts is reached within the specified time frame, the targeted account is locked. It remains locked for the length of time you set in the Failed login lockout duration field or until unlocked by the system administrator.
Failed login lockout duration	Specify the amount of time an account should be locked if it auto-locks due to failed logins. Maximum value is 1440 minutes; 0 means it should not auto-unlock. After this time, the account unlocks automatically. This does not affect accounts that have been locked manually. Administrators can unlock the account at any time.
UI Timeout Value	Specify the amount of time that must pass with no activity before the current session is forced to the login screen. For example, if this value is set to 30 minutes, the application automatically brings up the login screen after 30 minutes of inactivity, forcing you to log in again before you can resume your activities. A value of 0 means there is no limit.
Auto lock inactive accounts after	Set the ESM to lock user accounts that do not have administrator rights after a specific number of days of inactivity. The maximum value is 365 days; the minimum is 0, which disables the feature. The lockout lasts until an administrator unlocks the account.
Active sessions by one user	Set the number of active sessions a single user can have at one time. Maximum is 10; 0 disables the restriction.
Show Last User ID upon Login	Select whether you want the user name field populated with the one used on the last successful login.
ACL Settings	Select if you want to set up a list of IP addresses that are allowed to access your system or are blocked from your system.

Define logon password settings

There are several settings that you can define for the system logon password.

Before you begin

You must have system administrator rights.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Login Security**.
- 2 Click the **Passwords** tab, make your selections, then click **Apply** or **OK**.

Table 3-130 Option definitions

Option	Definition
Require advanced password	Select if you want the system to require that all passwords meet the following character and length requirements. At least: <ul style="list-style-type: none"> • 15 characters long • 2 numbers • 2 punctuation marks or symbols • 2 lowercase letters • 2 uppercase letters • Can't include 4 or more consecutive repeating characters If a password doesn't meet these requirements, it isn't accepted.
Password expiration	Specify how often the login password must be changed. The range is 0 to 365 days. If 0 is selected, the password doesn't expire.
Notification prior to password expiration	Select how many days prior to password expiration the user should be reminded to change their password. Maximum value is 30; minimum value is 1.
Password expiration grace period	Select the time period after a user's password has expired that the user can still log on. After the grace period, the account is locked and must be unlocked by the administrator.
Grace period logins	Select how many times a user can log on within the time period you specified after their password has expired. After the grace logins, the account is locked and must be unlocked by the administrator.
Password history count	Designate whether a history of passwords used by an individual should be stored on the system, and how many should be stored for each user. The range is 0 to 100 passwords. If it is set at 0, a history is not stored. If there is a history, it is checked when a user changes a password. If it is not unique, an error is returned and that password is not updated. If it is unique, the password is changed and a new history entry is added. If the storage limit is reached, the oldest password is deleted.
Restrict password changes once every	Restrict how frequently a user can change their password. For example, if you select 12, users are not allowed to change their passwords more than once within 12 hours.

Configure RADIUS authentication settings

Configure the ESM to authenticate users to a RADIUS server.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Login Security**.
- 2 Select the **RADIUS** tab, then fill in the fields for the primary server. A secondary server is optional.
- 3 Click **OK** or **Apply**.

When the server is enabled, all users except the system administrator authenticate with the RADIUS server. If authentication is disabled, users who are set up for RADIUS authentication can't access the ESM.

Table 3-131 Option definitions

Option	Definition
Enabled	Select to enable RADIUS authentication. When it is enabled, all users, except the system administrator, authenticate with the RADIUS server. If authentication is disabled, users who are set up for RADIUS authentication are not able to access the system.
Primary and Secondary Server IP Address	Enter the RADIUS server's IP address. A secondary server IP address, server port, and shared secret are not required.
Primary and Secondary Server Port	Enter the RADIUS server's port.
Primary and Secondary Shared Secret	Enter the shared secret (like a password) for your RADIUS server.

Set up the access control list

Set up a list of IP addresses that can be allowed to access or blocked from accessing your ESM.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Login Security**.
- 2 Click **ACL Settings**, then add IP addresses to the list.
- 3 Click **OK** to save the settings and close the **Access Control List**.

You can edit or remove IP addresses from the ACL list.

Table 3-132 Option definitions

Option	Definition
Allow these addresses	Select if you want to allow the IP addresses to access your system.
Deny these addresses	Select if you want to block the IP addresses from your ESM.
IP address/mask table	View the IP addresses that have been added to the list.
Add	Click to add an IP address or mask to the list.
Edit	Click to change the IP address that is highlighted on the list.
Remove	Click to delete the IP address that is highlighted on the list.

CAC settings

You can authenticate to the ESM by providing CAC credentials through the browser rather than by entering a user name and password.

CACs contain a client certificate that identifies the user, similar to the way a server certificate identifies a website. If you enable the CAC feature, we assume that you are familiar with CAC-based authentication. You know which browsers support this functionality and are familiar with the Electronic Data Interchange Personal Identifier (EDI-PI) associated with CACs.

Certificates are occasionally revoked. Certificate revocation lists (CRL) provide a way that systems can be made aware of these revocations. You can manually upload a .zip file containing CRL files.

ActivClient is the only supported CAC middleware on Windows. To use CAC authentication on the ESM from Windows using Internet Explorer, ActivClient must be installed on the client computer. Once ActivClient is installed, it is used to manage CAC credentials instead of the native Smart Card manager in Windows. The

ActivClient software is most likely already installed if the client accesses other CAC-enabled websites. Instructions on setting up ActivClient and where to go to download the software can be obtained at <http://militarycac.com/activclient.htm> or from your organization's intranet.



When relying on CAC validation for application authenticity, the security of the system is dependent on the security of the Certificate Authority (CA). If the CA is compromised, CAC-enabled logins are also compromised.

See also

[Configure CAC logon on page 198](#)

Configure CAC logon

To set up CAC logon, you must upload the CA root certificates, enable the CAC logon feature, and enable a CAC user by setting the user name to the card holder's Fully Qualified Distinguished Name (FQDN). Card holders can then access the ESM in a CAC-enabled browser without being prompted for a user name or password.




ESM supports the Gemalto and the Oberthur ID One card readers. Call Technical Support if you need assistance with your card reader.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Upload the CA root certificate.
 - a On your computer's control panel, click **Internet Options** | **Content** | **Certificates** | **Trusted Root Certification Authorities**.
 - b Select your current Root CA, then click **Export**.
 - c On the **Certificate Export Wizard**, click **Next**, then select **Base-64 encoded X.509** and click **Next**.
 - d Enter the location and name for the file you are exporting, click **Next**, then click **Finish**.
 - e On the system navigation tree of the ESM console, access **System Properties**, click **Login Security**, then select the **CAC** tab.
 - f Click **Upload**, then browse to the file that you exported and upload it to the ESM.
- 2 On the **Login Security** | **CAC** tab, enter the information and make the selections requested, then click **OK**.
- 3 Enable each CAC user.
 - a On **System Properties**, click **Users and Groups**, then enter the system password.
 - b In the **Users** table, highlight the name of the user, then click **Edit**.
 - c Replace the name in the **Username** field with the FQDN.
 - d (Optional) Enter the user's name in the **User Alias** field, then click **OK**.

Table 3-133 Option definitions

Option	Definition
CAC Mode is currently set to	<p>Select the Common Access Card (CAC) mode. The options are:</p> <ul style="list-style-type: none">• OFF — This is the default setting. CAC login is disabled so users have to log in using the ESM login prompt.• OPTIONAL — CAC authentication is available, but if the user does not provide a certificate, the ESM login prompt is shown as if CAC mode were off.• REQUIRED — Only CAC-enabled logins can access the system. The login prompt is never shown. If you select this option, enter a security PIN in Required Mode Security PIN (IPv4). This is the PIN you enter on the LCD panel if you need to switch the CAC mode to OPTIONAL if all users get locked out of the system. The PIN must be in IPv4 format (10.0.0.0) because it is recognized by the LCD panel. <div> Certificates and certificate authorities expire, so REQUIRED mode could potentially lock all users out of the ESM. A fail-safe button is located on the LCD panel on the front of the ESM, which switches CAC mode back to OPTIONAL.</div>
Certificate Credentials	Upload the chain of CA root certificates so the ESM has access to them. You can view the certificate file or download it to a location you select.
Certificate Revocation List	Upload the list of certificates that have been revoked or download them to a location you select.
Set up retrieval schedule	Set up an automatic retrieval schedule by typing the URL address and the frequency with which the ESM should poll for revocation file updates.

See also[CAC settings on page 197](#)**Configure Active Directory authentication settings**

You can configure the ESM to authenticate users to an **Active Directory**. When it is enabled, all users, except the system administrator, authenticate with the **Active Directory**. If authentication is disabled, users who are set up for **Active Directory** authentication can't access the system.

Before you begin

- Set up an **Active Directory** that can be accessed from the ESM.
- Create a group (see *Set up user groups*) with the same name as the **Active Directory** group that has access to the ESM. For example, if you name the group "McAfee Users," you must go to **System Properties | Users and Groups** and add a group named "McAfee Users."

Task



For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Login Security**.
- 2 Click the **Active Directory** tab, then select **Enable Active Directory Authentication**.
- 3 Click **Add**, then add the information requested to set up the connection.
- 4 Click **OK** on the **Active Directory Connection** page.

Table 3-134 Option definitions

Option	Definition
Enable Active Directory Authentication.	Select or deselect to enable or disable user authentication through your active directory. If you deselect authentication, users who are set up for active directory authentication can't access the system.
Add	Click to set up the connection with your active directory.
Edit	Make changes to the domain you select on the list.
Delete	Delete the domain you select on the list.

Table 3-135 Option definitions

Option	Definition
Use as Default	Select if you want to use this domain as the default.
Domain Name	Type the domain name. <div>  When you log on to the system, you can use this domain name as the user name. If you log on using your user name, the domain that is designated as the default is used. </div>
Add button	Add IP addresses used for the Active Directory. <ul style="list-style-type: none"> Administration server — Select if this is the address for the administration server. If not, deselect it. <div>  One of the addresses you enter must identify the host where the administrator server is running. </div> IP Address — Type the IP address for the Active Directory. Port and LDAP Port — Change the defaults, if needed. Use TLS — Select to use TLS encryption protocol for the data.
Edit button	Change existing IP address settings.
Delete button	Delete an existing IP address.

Set up user credentials for McAfee ePO

You can limit access to a McAfee ePO device by setting up user credentials.

Before you begin

The McAfee ePO device must not be set up to require global user authentication (see **Set up global user authentication**).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation bar of the ESM console, click **options**, then select **ePO Credentials**.
- 2 Click the device, then click **Edit**.




If the status column for the device says **Not Required**, the device is set up for global user authentication. You can change the status on the **Connection** page for the device (see *Change connection with ESM*).

- 3 Type the user name and password, test the connection, then click **OK**.

To access this device, users need the user name and password you added.

Table 3-136 Option definitions

Option	Definition
Table	View the McAfee ePO devices on the ESM. If the Status column says Not Required , the device is set up for global user authentication. If it says No Credentials , the device is set up to require individual user authentication. <div>  To change the user authentication setting, go to the Properties dialog box for the McAfee ePO device, click Connect, and change the setting in the Require User Authentication field. </div>
Edit	Click to add or change the credentials required for an individual to access the selected McAfee ePO device. Type the user name and password, then click Test Connection .
Delete	Click to delete the credentials for the selected device. You are asked to confirm.

Disable or re-enable a user

If a user exceeds the allowed failed login attempts within the timeframe set in **Login Security**, use this feature to re-enable the account. You might also use this feature if you need to block user access temporarily or permanently without deleting the user from the system.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties | Users and Groups**.
- 2 In the **Users** table, highlight the user name, then click **Edit**.
- 3 Select or deselect **Disable account**, then click **OK**.

The icon next to the user name on **Users and Groups** reflects the status of the account.

Authenticate users to an LDAP server

You can configure the ESM to authenticate users to an LDAP server.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Login Security**.
- 2 Click the **LDAP** tab.
- 3 Fill in the fields, then click **Apply** or **OK**.

When it is enabled, all users, except the system administrator, must authenticate with the LDAP server. If authentication is disabled, users who are set up for LDAP authentication can't access the system.

Table 3-137 Option definitions

Option	Definition
Enable	If you want all users, except the system administrator, to authenticate with the LDAP server, select Enable . If authentication is disabled, users who are set up for LDAP authentication can't access the system.
IP Address	Type the IP address for the LDAP server.
Port	Change the port for the server, if needed.
Use TLS or Use SSL	Select if you want to use an encryption protocol for the data.

Table 3-137 Option definitions *(continued)*

Option	Definition
Base Domain Name	Type the domain to be checked for credentials.
Group Attribute	Attribute where the user's group information is stored. Usually, this field does not need to be changed.
Group Filter	Filter that is used to collect group information. You can include or exclude specific groups from the search results.
User Filter	Filter that is used to collect user information. You can include or exclude specific users from the search results.

Set up user groups

Groups consist of users who inherit the settings of the group. If you have **User Administrator** privileges, you can add groups and assign devices, policies, and rights to them.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, click **System Properties | Users and Groups**, then type your password.
- 2 To the right of the **Groups** table, click **Add**, then fill in the information requested on each tab.
- 3 Click **OK**, then type your password again.

The group is added to the **Groups** table on the **Users and Groups** page.

Table 3-138 Option definitions


Option	Definition
Name and Description	Enter the name for this group and a description.
Users	Select the users to be part of this group.
Privileges	Select the privileges associated with this group. When you highlight a privilege, you can see a description in the Description box.
Devices	Select the devices that users can access. If you select all devices, users also have access to new devices when they are added to the system.
Policies	Select the policies that users can use and modify.
IP Address Filters	To restrict users' access to only report or alarm data for specific IP addresses, click Add and enter the address.
Zones	Select zones that users can access and modify.
Event Forwarding	<p>Select event forwarding destinations users can access and modify. This defines the devices where a user can forward events, if this group also has the event forwarding privilege, as well as the filters that specify the types of events that are forwarded. When you add an event forwarding destination to a specific user, it is added to all groups this user is a member of, as long as the groups have the event forwarding privilege.</p> <div>  <p>If an event forwarding destination does not belong to an access group, it has access to all devices.</p> </div>
Group Time Restrictions	Add day and time restrictions to limit the group's access to the ESM.

Table 3-138 Option definitions *(continued)*

Option	Definition
Reports	Select reports that users in this group can view and modify. The group must have the Reports privilege.
Views	Select the views that users in this group can view and modify. You can also share visibility with other users and groups.
Watchlists	Select the watchlists that users in this group can view and modify. You can also share visibility with other users and groups.
Filters	Select the filter sets that users in this group can see, modify, or both.

Table 3-139 Option definitions

Option	Definition
Table	Lists all the users that have been added to the system. Select the users you want in this group.
Select All	Selects all the users. You can then deselect users that are not part of the group.
Select None	Deselects all the users. You can then select the ones you want in this group.

Table 3-140 Option definitions


Option	Definition
Limit access of this group	Limits the rights for the group.
Privileges list	Lists all the rights available on the ESM. Select or deselect them individually or click Select All or Select None . <div>  If you have User Administration rights, you can unlock or change the rights of standard users, not administrators. </div>
Description	Displays a description of the selected privilege.

Table 3-141 Option definitions



Option	Definition
(Views only) Inherit permissions from parent folder	<div>  You must have Master or Administrative rights to enable or disable this option. </div> <p>Selected by default. If you don't want the permissions to be inherited from the parent, deselect this option. The Groups and Users tabs become active.</p>
(Reports and Watchlists only) Inherit modify settings	<div>  You must have Master or Administrative rights to enable or disable this option. </div> <p>Selected by default. The users inherit Modify rights. Deselect this option if you want to change the default settings.</p>

Table 3-141 Option definitions *(continued)*


Option	Definition
Groups tab	<p>Lists all groups that you have access to, based on the groups you are a member of. Indicate the groups that must have access to the items you have selected. You can select Read only, Modify, or neither. If you don't select either of them, the group has deny rights. If you select Modify, Read only is selected automatically.</p> <p>A pseudo group called Default is shown for Master or Administrative users. Groups created in the future get this privilege.</p>
Users tab	<p>Lists all users that you have access to, based on the groups you are a member of. Indicate the users that must have access to the items you have selected. You can select Read only, Modify, or neither. If you don't select either of them, the user has deny rights. If you select Modify, Read only is selected automatically.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin: 10px 0;">  User rights take precedence over group rights. For example, if a user is given only Read access to a resource, but their group is given Modify access, the user can only Read the selected items. </div> <p>You can add users to the list or remove them.</p> <ol style="list-style-type: none"> 1 Click Add, click the users, then click OK. 2 For each user, select Read or Modify, then click OK. <p>If a user is not on the list, the system uses the group rights of that user. If a user is on the list but doesn't have Read or Modify checked, that user has explicit deny rights to that resource.</p>

Table 3-142 Option definitions

Option	Definition
Policies list	Lists the policies on the ESM. Select the policies that this group can access.
Select All	Selects all the policies.
Select None	Deselects all the policies.

Table 3-143 Option definitions

Option	Definition
List	View the IP addresses on the list.
Add	Click to add an IP address to the list.
Edit	Modify the selected IP address.
Remove	Delete the selected address from the list.

Table 3-144 Option definitions

Option	Definition
Zones list	Lists the zones that have been added to the ESM. Select the zones this group can access.
Select All	Selects all the zones on the list.
Select None	Deselects all the zones on the list.

Table 3-145 Option definitions


Option	Definition
Event forwarding destinations list	Lists the destinations that were added to the ESM. Select the destinations this group can access. <div>  If a destination does not belong to an access group, it must have access to all devices. </div>
Select All	Selects all the destinations on the list.
Select None	Deselects all the destinations on the list.

Table 3-146 Option definitions

Option	Definition
Enable restrictions	Select to activate restrictions for this group.
Time zone	Select the time zone this group is in.
Start time and End time	Select the time of day that the groups access starts and ends. If they should have access 24 hours on the selected days, select 00:00 in both fields.
Days of the week	Select the days of the week the group members can access the ESM.

Table 3-147 Option definitions

Option	Definition
Name column	Lists the reports on the ESM.
Read column	Select the reports that this group should be able to read. If you select Modify , Read is also selected.
Modify column	Select the reports that this group should be able to modify.
Share	Click to select other groups or users to share visibility of the selected reports.

Table 3-148 Option definitions

Option	Definition
Name column	Lists all the views on the ESM.
Read column	Select the views that this group should be able to read.
Modify column	Select the views that this group should be able to modify.
Share	Click to select other groups or users to share visibility of the selected items.

Table 3-149 Option definitions


Option	Definition
Name column	Lists all the watchlists on the ESM.
Read column	Select the watchlists that this group should be able to read. If you select Modify , Read is also selected.
Modify column	Select the watchlists that this group should be able to modify.
Share	Click to select other groups or users to share visibility of the selected items.

Add a group with limited access

To restrict specific users' access to features on the ESM, create a group that includes those users. This option limits their access to alarms, case management, ELM, reports, watchlists, asset management, policy editor, zones, system properties, filters, and the actions toolbar (see *Working with users and groups*). All other features are disabled.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Users and Groups**, then type the system password.
- 3 Do one of the following:
 - If the group is already set up, select it on the **Group** table, then click **Edit**.
 - If you are adding a group, click **Add** next to the **Groups** table, fill in the name and description, then select users.
- 4 Click **Privileges**, then select **Limit access of this group**.

Most privileges are disabled.
- 5 From the remaining list of privileges, select the privileges that you want this group to have.
- 6 Click each tab and define the rest of the settings for the group.

Backing up and restoring system settings

Save current system configuration settings automatically or manually so they can be restored in case of system failure or data loss. You can also set up and save current settings to a redundant ESM.

A standard backup saves all configuration settings, including those for policy, SSH, Network, and SNMP files. When you add an ESM device, **Backup & Restore** is enabled to back up every 7 days.

You can back up events, flows, and logs received by the system. The first backup of event, flow, or log data saves only data from the start of the current day. Subsequent backups save data starting at the time of the last backup.

To restore the system, select backup files on the ESM, a local computer, or a remote location to revert your settings and data to a previous state. When you perform this function, all changes made to the settings after the backup was created are lost. For example, if you are performing a daily backup and want to restore the data from the last three days, select the last three backup files. The events, flows, and logs from the three backup files are added to the events, flows, and logs that are currently on the ESM. All settings are then overwritten with the settings contained in the most recent backup.

See also

[Back up ESM settings and system data on page 206](#)

[Restore ESM settings on page 208](#)

[Restore backed up configuration files on page 208](#)

[Work with backup files on ESM on page 209](#)

[Manage file maintenance on page 209](#)

Back up ESM settings and system data

Back up and save the ESM configuration files before you start any software upgrades.

When you add an ESM device, **Backup & Restore** is enabled to back up every seven days. You can disable it or changes the default settings. See KB article, [Backup process for McAfee \[ESM\] devices](#) for details.

We recommend you make a **Full Backup** of all devices before you start an upgrade. A full backup contains:

- Settings for the ESM, ERC, DEM, ADM, and ACE devices.



ELM full backups only include configuration settings. The database settings must be backed up separately or you lose all database connections to your local shares, remote shares, and SANs.

- Stop CPService and then DBServer and create a copy of the contents of: /usr/local/ess/data/, /etc/NitroGuard, and other folders on a remote share.

If anything goes wrong during the upgrade, you can:

- Reinstall the software to the existing version.
- Reinstall the backup files.
- Try upgrading to the next version again.



Backups are only compatible with the current version of the ESM device. You can't install a backup of a previous version on an upgraded ESM device.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- On the system navigation tree, select **System Properties**, then click **ESM Management** | **Maintenance** | **Backup**.
- Define the settings for the backup.
- Click **OK** to close the **Backup & Restore** page.

Table 3-150 Option definitions

Option	Definition
Backup Frequency	When new ESM devices are added to the system, the Backup & Restore function is enabled to perform a backup every seven days. You can change the frequency or disable backup.
Backup Data For	Select what you want to include in the backup.
Backup Location	Select where you want the backup saved: <ul style="list-style-type: none"> ESM — It is saved on the ESM and accessed on the File Maintenance page. Remote Location — It is saved in the location you define in the fields that become active. If you are saving a copy of the ESM and all system data manually, you must select this option. <div> When you back up to a CIFS share, use a slash (/) in the remote path field. </div>
Backup Now	Manually back up ESM settings and events, flows, and logs (if selected). Click Close when the backup is completed successfully.
Full Backup Now	Manually save a copy of the device settings and the system data. This can't be saved to the ESM, so you must select Remote Location in the Backup Location field and enter the location information. <div> We highly recommended you make a full backup before any major version update to avoid data loss. </div> <div> Using the Common Internet File System (CIFS) share type with Samba server versions greater than 3.2 can result in data loss. </div>

See also

[Backing up and restoring system settings on page 206](#)

[Restore ESM settings on page 208](#)

[Restore backed up configuration files on page 208](#)

[Work with backup files on ESM on page 209](#)

[Manage file maintenance on page 209](#)

Restore ESM settings

When the system fails or there is data loss, you can restore your system to a previous state by selecting a backup file.

Task

If the database contains the maximum allowed records and the records being restored are outside of the range of current data on the ESM, the records are not restored. To save and access data outside of that range, you must have inactive partition archiving set up.

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **ESM Management | Maintenance | Restore Backup**.
- 2 Select the type of restore you need to perform.
- 3 Select the file you want to restore or enter the information for the remote location, then click **OK**.

Restoring a backup can take a long time, based on the size of the restore file. The ESM is offline until the full restore is completed. During this time, the ESM tries to reconnect every 5 minutes. When the process is completed, the **Login** page appears.

See also

[Backing up and restoring system settings on page 206](#)

[Back up ESM settings and system data on page 206](#)

[Restore backed up configuration files on page 208](#)

[Work with backup files on ESM on page 209](#)

[Manage file maintenance on page 209](#)

Restore backed up configuration files


You can restore SSH, Network, SNMP and other configuration files that were backed up on the ESM for each device.

Before you begin

Back up configuration files on the ESM (see [Back up ESM settings and system data](#)).

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click the device, then click the **Properties** icon .
- 2 Click the **Configuration** option for the device, click **Restore Config**, then click **Yes** on the confirmation page.

See also

[Backing up and restoring system settings on page 206](#)

[Back up ESM settings and system data on page 206](#)

[Restore ESM settings on page 208](#)

[Work with backup files on ESM on page 209](#)

[Manage file maintenance on page 209](#)

Work with backup files on ESM

The backup files that were saved to the ESM can be downloaded, deleted, or viewed. You can also upload files to add them to the list of backup files.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **File Maintenance**.
- 2 In the **Select Type** drop-down list, select **Backup Files**.
- 3 Select the action you want to perform.
- 4 Click **OK**.

See also

[Backing up and restoring system settings on page 206](#)

[Back up ESM settings and system data on page 206](#)

[Restore ESM settings on page 208](#)

[Restore backed up configuration files on page 208](#)

[Manage file maintenance on page 209](#)

Manage file maintenance

The ESM stores backup, software update, alarm log, and report log files. You can download, upload, and remove files from each of these lists.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **File Maintenance**.
- 2 In the **Select File Type** field, select **Backup Files**, **Software Update Files**, **Alarm Log Files**, or **Report Files**.
- 3 Select the files, then click one of the options.
- 4 Click **Apply** or **OK**.

Table 3-151 Option definitions

Option	Definition
Select File Type	Select the type of file you want to manage.
Download	Save the selected file to a location not on the ESM.
Upload	Add a file to the ESM.
Remove	Delete the selected file so it is no longer on the ESM.
Refresh	Refresh the list of files to reflect recent changes.
Details (only for backup files)	View details for the selected backup.
Settings (only for backup files)	Access the Backup & Restore page.

See also

Backing up and restoring system settings on page 206

Back up ESM settings and system data on page 206

Restore ESM settings on page 208

Restore backed up configuration files on page 208

Work with backup files on ESM on page 209

Setting up redundant ESMs

Save ESM settings to another ESM that can be converted to the primary ESM in case of system failure or data loss.



The ESM redundancy feature is not available on McAfee Event ReceiverSMREC combo devices.

See also

Set up ESM redundancy on page 210

Remove a redundant ESM on page 211

Set up ESM redundancy

To save your system settings on a redundant ESM, you must set up each ESM so that they communicate with each other. The system settings are synced every five minutes. Data tables are synced if you set up the primary ESM to do so.

Before you begin

The primary and each redundant ESM must be installed and configured.

The current user must have administrative privileges. ([System Properties](#) | [Users and Groups](#) | [Edit](#))

Each ESM must have SSH enabled. ([System Properties](#) | [Network Settings](#) | [Enable SSH](#))

Task

- 1 Log on to the primary ESM.
- 2 In **System Properties**, click **ESM Management** | **Configuration tab** | **Redundancy**.
- 3 Select **Shared Queries** unless you have a specific reason to disable it.
- 4 If you want to sync data tables, select **Schedule Sync**, then select when you want the sync to occur in the **Sync Time** field.
- 5 In the **SSH Port** field, select the SSH port the devices use to communicate.



All ESMs in the redundancy group must use the same SSH port.

- 6 Add the redundant ESM(s) to the primary ESM.



You can add up to five redundant ESMs.

- a Click **Add**, then type a name for the redundant ESM.
- b Type the IP address, user name, and password for the redundant ESM, then click **Next**.

The primary ESM attempts to communicate with the redundant ESM(s) and displays a status message.



The this screen does not refresh. to see updated data, close and re-open the screen.

- c Click **Finish**.

- 7 Click **OK**.

The primary and redundant ESM begin to sync. System settings are synced every five minutes.

See also


[Setting up redundant ESMs on page 210](#)

[Remove a redundant ESM on page 211](#)

Remove a redundant ESM

Remove an ESM from the list of redundant ESMs communicating with the primary ESM.

Task

- 1 On the system navigation tree, click the **System Properties** icon , and then click **ESM Management | Configuration tab | Redundancy**.
- 2 On the table of redundant ESMs, verify that the status of the ESM to be removed is **Redundant OK** or **Lost communication**.



If the status is **Syncing**, do not remove the redundant ESM.

- 3 Select the ESM, then click **Remove**.

The redundant ESM is removed from the list and is no longer available to receive backup data from the primary ESM. Other ESMs on the list continue to sync with the primary ESM.

See also

[Setting up redundant ESMs on page 210](#)

[Set up ESM redundancy on page 210](#)

[Remove a redundant ESM on page 211](#)

Enabling and disabling shared queries


The shared queries feature reduces the load on the primary ESM in a redundant system.

The reduction is accomplished by running queries on redundant ESMs when the query's specified date range indicates that the query data is present on a redundant ESM.

This feature effectively uses the resources provided by redundant ESMs. When **Shared Queries** is enabled, queries are sent to the redundant ESM if the requested data spans more than 30 days or the query started more than 12 hours ago. The results of these queries are always returned to the primary ESM.

Shared Queries is enabled by default. Older model ESMs might take longer to process queries; to reduce processing time, disable this feature.

Task


- 1 On the system navigation tree, select the ESM, then click the **Properties** icon .
- 2 Click **ESM Management** | **Configuration tab** | **Redundancy**.
- 3 On the **Redundancy Configuration** page, deselect **Shared Queries**, then click **OK**.

A CPService restart is performed.

Change redundant ESM to primary ESM

If the primary ESM fails or needs to be deactivated, change the redundant ESM to primary.


Task

- 1 On the navigation tree, select the redundant ESM and then click the **Properties** icon .
- 2 Click **ESM Management** | **Configuration tab** | **Redundancy**.
- 3 Select the redundant ESM and then click **Fail-Over**.
When the change is complete, a status message appears.
- 4 When prompted, type the password for the redundant ESM that is changing to primary ESM.

Managing the ESM

You can perform several operations to manage the software, logs, certificate, feature files, and communication keys for the ESM.

Tab	Option	Definition
Configuration	Manage Logs	Configure the types of events that are logged on the event log.
	ESM Hierarchy	Configure data options when working with hierarchical ESM devices.
	Obfuscation	Define global settings to mask selected data on any alert record that is sent out in event forwarding or sent to a parent ESM.
	Logging	Send internal events to the ELM for storage. This data can be used for auditing.
	System Locale	Select the system language to use for logging events such as health monitor and device log.
	Name Map	Deselect the ports and protocols to have them display raw numbers instead of names. For example, if you deselect Source Port or Destination port , <i>http:80</i> is displayed as <i>80</i> . If you select <i>Protocols</i> , raw number <i>17</i> is displayed as <i>udp</i> .
	Local Network	Add a list of the IP addresses or subnets included in your Local Network.
Key Management	Redundancy	Set up one or more redundant ESMs to back up all the data on the primary ESM (see <i>Redundant ESM</i>).
	Certificate	Install a new Secure Socket Layer (SSL) certificate.
Maintenance	Regenerate SSH	Regenerate the private or public SSH key pair to communicate with all devices.
	Update ESM	Update ESM software from the McAfee rules and updates server or a McAfee security engineer.
	ESM Data	Download a .tgz file that contains information regarding the status of the ESM. This status can assist McAfee Support troubleshoot and resolve issues.

Tab	Option	Definition
	Task manager	View the queries running on the ESM and stop them, if needed.
	Shutdown	Shut down the ESM. You are warned that this action causes all users to lose communication with the ESM.
	Reboot	Stop and restart the ESM. You are warned that this action causes all users to lose communication with the ESM.
	Get Features	If you have purchased additional features, enable them on your ESM by downloading an encrypted file that contains information about features that your ESM supports.
	Set Features	Install the file you downloaded with Get features .
	Connect	Give McAfee support access to your system when you call for support. <div>  This option is not FIPS-compliant and is not available when operating in FIPS mode. </div>
	View Statistics	Access the following information for any ESM device: <ul style="list-style-type: none"> • Memory and swap space utilization statistics. • CPU utilization. • System switching activity. • Input/output and transfer rate statistics. • Queue length and load averages.

Manage logs

There are several types of events that are generated on the ESM. You can select the ones you want saved in the event log.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **ESM Management**.
- 2 Click **Manage logs**, then select the event types you want to log.
- 3 Click **OK**.

Tab	Option	Description
Configuration tab	Manage Logs	Configure the types of events that are logged on the event log.
	ESM Hierarchy	Configure data options when working with hierarchical ESM devices.
	Obfuscation	Mask selected fields on any alert record that is sent out in event forwarding or sent to a parent ESM.
	Logging	Send internal events to the ELM for storage. This data can be used for auditing purposes.
	System Locale	Select the language for event logs such as the health monitor log and device log.
	Name Map	Deselect the ports and protocols to have them display raw numbers instead of names. For example, if you deselect Source Port or Destination port , <i>http:80</i> is displayed as <i>80</i> . If you select Protocols , raw number <i>17</i> is displayed as <i>udp</i> .


Tab	Option	Description
	Local Network	Add a list of the IP addresses or subnets included in your Local Network.
	Redundancy	Set up one or more redundant ESMs to back up all the data on the primary ESM (see <i>Redundant ESM</i>).
Key Management tab	Certificate	Install a new SSL certificate.
	Regenerate SSH	Regenerate the private or public SSH key pair to communicate with all devices. When the key is regenerated, it replaces the old key pair on all devices managed by the ESM.
Maintenance	Update ESM	Update ESM software from the McAfee rules and updates server or a McAfee security engineer.
	ESM Data	Download a .tgz file that contains information regarding the status of the ESM. This status can assist McAfee Support troubleshoot and resolve issues.
	Task Manager	View and manage the queries that are running on the ESM.
	Shutdown	Shut down the ESM. You are warned that this action causes all users to lose communication with the ESM.
	Reboot	Start the ESM. You are warned that this action causes all users to lose communication with the ESM.
	Get Features	To enable newly purchased ESM features, first download an encrypted file that contains information about your currently supported ESM features.
	Set Features	Install the file you downloaded with Get features .
	Connect or Disconnect	Give Technical Support access to your system when you call McAfee for support. <div>  This option is not FIPS-compliant, so is not available when operating in FIPS mode. </div>
	View Statistics	Access the following information for any ESM device: <ul style="list-style-type: none"> • Memory and swap space utilization statistics. • CPU utilization. • System switching activity. • Input/output and transfer rate statistics. • Queue length and load averages.
	Backup	Back up the ESM settings now or set up auto backup. The backup can be stored on the ESM or in a remote location. You can also restore your system settings to a previous backup.
	Restore Backup	Back up events, flows, and logs now or set up auto backup. You can also restore the events, flows, and device logs for the date range you specify.

Table 3-152 Option definitions

Option	Definition
Specify which event log types	Select or deselect types to specify the types of event logs that you want collected by this ESM. When you click on a type, a description is shown.

Mask IP addresses

You can select to mask specific data on event records sent out in event forwarding or to a parent ESM.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the system navigation tree, select **System Properties**, then click **ESM Management** | **ESM Hierarchy**.
- 2 Select **Obfuscate** for the ESMs that you want to mask data on.
The **Obfuscation Fields Selection** page opens.
- 3 Select the fields that you want to mask.
- 4 Click **OK**.

Once this is set up, if a parent ESM requests a packet from a child ESM, the data you selected is masked.

Table 3-153 Option definitions

Option	Definition
Specify which event log types	Select or deselect types to specify the types of event logs that you want collected by this ESM. When you click on a type, a description is shown.

Table 3-154 Option definitions

Option	Definition
Available for obfuscation list	Lists the fields that can be hidden. This list includes fields that might contain sensitive data and all custom types. To locate a field on the list, type the name in the search field.
Selected fields list	Lists the fields that are currently hidden.
Arrows	Moves the selected fields from one list to the other.
Configure global obfuscation settings link	Click to add or change the obfuscation settings for the system.

Table 3-155 Option definitions

Option	Definition
Seed value	To make sure that obfuscation is performed the same way each time, enter a seed in the Seed value field, or click Generate to generate a random seed. This is useful if you obfuscate IP addresses across multiple ESMs and want to keep the values synchronized.
Include local network	Select to hide IP addresses inside and outside your local network. This extends to IP custom types such as IPv4 and IPv6 addresses.
Modify local network settings	Click to edit the IP addresses on your local network.

Table 3-156 Option definitions

Option	Definition
Local Network field	Enter a list of the IP addresses or subnets included in your Local Network, separated by commas. The field allows a maximum of 2,000 characters. If your Local Network is longer than that, you can consolidate multiple subnets into a shorter Local Network using Classless Inter-Domain Routing (CIDR) notation.

Set up ESM logging

If you have an ELM device on your system, you can set up the ESM so the internal event data it generates is sent to the ELM device. To do so, you must configure the default logging pool.

Before you begin

Add an ELM device to your system.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the system navigation tree, select **System Properties**, then click **ESM Management**.
- 2 On the **Configuration** tab, click **Logging**.
- 3 Make the requested selections, then click **OK**.

Table 3-157 Option definitions

Option	Definition
Log Configuration page	Select Logging .
Device - ELM association page	If you haven't associated an ELM with this ESM, you are asked if you want to. Click Yes .
Select ELM for Logging page	If you have more than one ELM device on the system, select the ELM you want to store the data on. This ESM always logs on to the ELM you select.
Select ELM IP Address page	Select the IP address you want the ESM to communicate with the ELM through. You are notified when the selected ELM is successfully associated with the device.
No ELM Pools page	If storage pools have not been configured on the ELM, you are informed that you need to add storage pools to the ELM before logging can be enabled.
ELM Logging Options page	Select the storage pool the data must be logged.

Regenerate SSH key

Regenerate the private or public SSH key pair to communicate with all devices.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the system navigation tree, select **System Properties**, then click **ESM Management**.
- 2 On the **Key Management** tab, click **Regenerate SSH**.
You are warned that the new key replaces the old key.
- 3 Click **Yes**.

When the key is regenerated, it replaces the old key pair on all the devices managed by the ESM.


Queries task manager

If you have administrator or master user rights, you can access the **Task Manager**, which displays the list of queries running on the ESM. From here, you can close specific queries if they affect system performance. Long running queries have a higher likelihood of affecting performance.



The intent of this feature is to troubleshoot ESM runtime issues, not to close queries. Use this feature with assistance from McAfee support.

Characteristics of the task manager include:

- You can close report, view, watchlist, execute and export, alarm, and external API queries on the system. You cannot close system queries.
- When you click a query, the details are displayed in the **Query Details** area.
- By default, the list refreshes automatically every five seconds. If you select a query and the list auto-refreshes, it remains selected and the details are updated. If the query is complete, it no longer appears on the list.
- If you do not want the list to auto-refresh, deselect **Auto refresh list**.
- To view system tasks, which are tasks that haven't been identified yet, deselect **Hide system tasks**.
- The columns on the table can be sorted.
- You can select and copy the data in the **Query Details** area.
- If a query can be closed, it has a delete icon  in the last column. When you click it, a dialog box requests confirmation.

Manage queries running on ESM

The **Task Manager** displays a list of the queries that are running on the ESM. You can view their status and delete any that affect system performance.

Task

For details about product features, usage, and best practices, click ? or **Help**.



- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **ESM Management**, click the **Maintenance** tab, then click **Task Manager**.
- 3 Review and take action on the list of running queries.

Table 3-158 Option definitions

Option	Definition
Table	View a list of the queries that are running on the ESM. The columns on the table can be sorted.
Query Details	View details for the task you select on the table. You can select and copy this text.
Hide system tasks	Deselect to view system tasks, which are tasks that haven't been identified yet.
Auto refresh list	Deselect if you do not want the list to refresh automatically every 5 seconds. If you select a query and the list auto-refreshes, it remains selected and the details are updated. If the query is complete, it no longer appears on the list.
	Click to kill the task.

Update primary or redundant ESM

If you are updating a primary or redundant ESM, you must follow specific steps to avoid losing the event, flow, and log data.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Disable the collection of events, flows, and logs.
 - a On the system navigation tree, select **System Information**, then click **Events, Flows, & Logs**.
 - b Deselect **Auto check every**.
- 2 Update the primary ESM.
- 3 Update the redundant ESM.
- 4 Enable the collection of events, flows, and logs by selecting **Auto check every** once again.



If the update fails, see *Update to version 9.3*.

Using a global blacklist

A blacklist is a way to block traffic as it flows through a network device before the deep packet inspection engine analyzes it.

You can use the network device **Blacklist** option to set up a blacklist for individual network devices on the ESM. With **Global Blacklist**, you can set up a blacklist that applies to all network devices managed by the ESM. This feature only allows permanent blacklist entries. To set up temporary entries, you must use the network device **Blacklist** option.

Each network device can use the global blacklist. The feature is disabled on all devices until you enable it.

The **Global Blacklist Editor** page includes three tabs:

- **Blocked Sources** — Matches against the source IP address of traffic passing through the device.
- **Blocked Destinations** — Matches against the destination IP address of traffic passing through the device.
- **Exclusions** — Provides immunity from being automatically added to either of the blacklists. Critical IP addresses (for example, DNS and other servers or system administrators' workstations) can be added to the exclusions. This ensures that they are never automatically blacklisted regardless of the events they might generate.



Entries in both **Blocked Sources** and **Blocked Destinations** can be configured to narrow the effect of the blacklist to a specific destination port.

When adding entries:

- **Add** is enabled when you change the IP address or the port.
- Entries in the **Blocked Sources** and **Blocked Destinations** lists can be configured to blacklist on all ports, or a specific port.

- Entries that use a masked range of IP addresses must be configured with the port set to any (0) and the duration must be permanent.
- While these lists require IP address format, there are a few tools included to help add meaning to these addresses. After typing an IP address or host name in the **IP Address** field, the button next to that control says either **Resolve** or **Lookup** based on the value entered. If it says **Resolve**, clicking it resolves the entered host name, populates the **IP Address** field with that information, and moves the host name to the **Description** field. Otherwise, clicking **Lookup** performs a lookup on the IP address and populates the **Description** field with the results of that lookup.



Some websites have more than one IP address, or have IP addresses that are not always the same. Don't rely on this tool to ensure blocking of some websites.

See also

[Set up a global blacklist on page 219](#)

Set up a global blacklist

Set up a global blacklist that is common to all the devices you select so you don't have to enter the same information on multiple device.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Global Blacklist**.
- 2 Select the **Blocked Sources**, **Blocked Destinations**, or **Exclusions** tab, then manage blacklist entries.

- 3 Select the devices that must use the global blacklist.
- 4 Click **Apply** or **OK**.

Table 3-159 Option definitions

Option	Definition
Blocked Sources tab	Manage the source IP addresses you want to block.
Blocked Destinations tab	Manage the destination IP addresses you want to block.
Exclusions tab	Manage the list of IP addresses that should never be blacklisted automatically, such as DNS and other servers, or the system administrator's workstation.
IP Address	When adding an item to a list, type the IP address.
Lookup	Click to look up the description for the IP address you entered.
Add	After typing the IP address, click to add it to the list.
Port	Type a port number if you want to narrow the effect of the blacklist to a specific destination port. The default setting is zero (0), which allows any port.
Modify	Change the description on an existing blacklist item, then click this option.
Description	(Optional) Enter a description for the IP address or click Lookup to locate a description. To change the description on an existing address, type the changes and click Modify .
Manage	Click to open a list of network devices on the ESM, then select the devices that should use the global blacklist.
Write icon	Click when you are ready to save the new items to the ESM. If you exit the blacklist page prior to writing the changes, they are not saved.
Read icon	Click to update blocked sources, blocked destinations, and exclusions.
Remove icon	Click to remove the selected item from the blacklist. The Status field will change to Delete on Next Write .
View Events icon	Click to generate a report of events from the offending IP addresses. The report will be displayed as a view on the console.

Table 3-160 Option definitions

Option	Definition
Table	View a list of the network devices on the ESM and whether or not global blacklist is enabled on each of them.
Enabled column	Select the devices that use global blacklist.

See also

[Using a global blacklist on page 218](#)

Data enrichment

You can enrich events sent by the upstream data source with context not in the original event, such as an email address, phone number, or host location information. This enriched data becomes part of the parsed event and is stored with the event just like the original fields.

Set up data enrichment sources by defining how to connect to the database and access one or two table columns within that database. Then define which devices receive the data and how to enrich that data, both events and flows.

You can also edit or remove data enrichment sources, as well as run a query on the **Data Enrichment** page.

Events that trigger on the ESM are not enriched. Data acquisition takes place on the ESM, not on the devices.

A connector to the relational data source in Hadoop HBase uses the key-value pairs from the source for enrichment. The identity mapping in HBase can be pulled to a Receiver regularly to enrich events.

See also

[Add data enrichment sources on page 221](#)

[Add Hadoop HBase data enrichment source on page 224](#)

[Add Hadoop Pig data enrichment source on page 225](#)

[Add Active Directory data enrichment for user names on page 225](#)

Add data enrichment sources

Add a data enrichment source and define which devices receive the data.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Data Enrichment | Add**.
Tabs and fields on the **Data Enrichment Wizard** vary based on the enrichment type you select.
- 2 On each of the tabs, complete the fields, then click **Next**.
- 3 Click **Finish**, then click **Write**.
- 4 Select the devices you want to write the data enrichment rules to, then click **OK**.

Table 3-161 Option definitions

Option	Definition
Add	Add a new data enrichment source.
Edit	Make changes to an existing source.
Remove	Remove an existing source.
Run Now	Run a query on the selected data enrichment source.
Enabled	Enable or disable the selected data enrichment source.
Write	Click to write the settings to the devices you selected on the Destination tab when adding or editing the sources.

Table 3-162 Option definitions

Tab	Option	Definition
Main tab	Name	Type a name for the source.
	Enable	Select whether to enable this source.
	Lookup Type	Select the data type to use for lookup.
	Enrichment Type	Select the data type you want to enrich.
	Pull Frequency	Select how often to execute this data enrichment source.

Table 3-162 Option definitions *(continued)*

Tab	Option	Definition
Source tab	<ul style="list-style-type: none"> CIFS, NFS, FTP, SFTP, and SCP source types can only use external files for enrichment. The other source types require you to write a query for a database or regular expression. The file you pull for data enrichment must be formatted as LookupValue=EnrichmentValue. Each entry must be on a separate line. For single column enrichment, only lookup value entries are needed. For two column enrichment, the lookup value must be separated from the enrichment value by an equal symbol (=). <p>For example, a file that uses IP address to host names might look like this:</p> <pre>10.5.2.3=New York 10.5.2.4=Houston</pre>	
	Type	Type of database driver for the source.
	Authentication	If Basic is selected, user name and password for the web site if it requires you to log on. Default setting is None .
	DB Name	Name of the database.
	Host	Name of the computer running the database.
	Ignore Invalid Certificates	If the web site you are trying to search is at an https URL, select this option to ignore invalid SSL certificates.
	IP Address	IP address of the database.
	Job Tracker Host	Apache Hadoop Job Tracker Host address or IP address. Not required; if blank, the system uses the Node Name Host.
	Job Tracker Port	Port where the Job Tracker Host listens. Not required; if blank, the system uses the Node Name Host.
	Method	If POST is selected, the post content or argument that might be required to navigate to the web page containing the content that you want to search on. Default setting is GET .
	Mount Point	Directory for the files.
	Node Name Host	Apache Hadoop Node Name Host address or IP address. Do not include protocol.
	Node Name Port	Port where the Node Name Host listens. Not required; if blank, the system uses the Node Name Host.
	Password	Password to access the database.
	Path	Path to the database. If you select FTP in the Type field, the path is relative to your home directory. To specify an absolute path on the FTP server, insert an extra forward slash (/) at the beginning of the path. For example, //var/local/path.
	Port	Port for the database.
	Share Name	Directory for the files.
	Username	The name of the user who can access the database. For LDAP, enter a fully-qualified domain name with no spaces. For example, uid=bob,ou=Users,dc=example,dc=com OR administrator@idahoqa.mcafee.com.

Table 3-162 Option definitions *(continued)*

Tab	Option	Definition
Parsing tab	Raw data	When HTTP/HTTPS is selected as the source type, view the first 200 lines of the HTML source code for the URL entered in the URL field on the Source tab. It is only a preview of the website, but is enough for you to write a regular expression to match on. A Run Now or scheduled update of the data enrichment source includes all matches from your regular expression search. This feature supports RE2 syntax regular expressions, such as <code>(\d{1,3}\.){1,3}\.(\d{1,3}\.){1,3}</code> .
	Header lines to skip	Typically, an Internet site has header code that you are not interested in searching. Specify how many lines from the top of the site you want to skip so that the search doesn't include header data.
	New line delimiter	Type what is used on the site to separate the values you are interested in. This field has a default of <code>\n</code> , which indicates that a new line is the delimiter. The other most common delimiter is a comma.
	Ignore Expression	Type a regular expression that removes any unwanted values from the results of your regular expression search.
	Regular Expression	(Required) Type the logic used to find a match and extract the values from the site. The most common use cases are to create an expression that matches on a list of known malicious IP addresses or MD5 sums listed on a site. If you provided two match groups in your regular expression, you can map the results of each regex match to Lookup Value or Enrichment Value .
	Lookup Value or	The value to look for in events collected from the ESM where you want to add more values. It maps to the Lookup Field on the Destination tab.
	Enrichment Value	The value that is enriched or inserted into the source events that match on the lookup value. It maps to the Enrichment Field on the Destination tab.
Query tab	Set up the query for Hadoop HBase (REST), Hive, LDAP, MSSQL, MySQL, Oracle, PIG, or McAfee Real Time for McAfee ePO types.	
Scoring tab	Set the score for each value that is returned on a single column query. Select the source and target field you want to score on, then click Run Query .	
	Value	Shows the returned values.
	Score	Shows the numeric stepper that you can use to set the risk score for that value. Make changes if needed, then click Update List .
Destination tab	View the devices and the rule for field mapping for the devices that this data enrichment source populates.	
	Add	Select the devices and rules.
	Edit	Change the devices or the rules settings.
	Remove	Delete a device and rule setting.

Table 3-163 Option definitions

Option	Definition
Lookup Field	Select the field it should be looked up by.
Enrichment Field	Select the field to be enriched.
Use Static Value	Select if you want to use a static value.

Table 3-163 Option definitions *(continued)*

Option	Definition
Enrichment Value	If you selected Use Static Value , you must enter the enrichment value.
Modify Severity	Select if you want to use severity as an enrichment field, then select the percent that you want to increment or decrement by.

See also[Data enrichment on page 220](#)[Add Hadoop HBase data enrichment source on page 224](#)[Add Hadoop Pig data enrichment source on page 225](#)[Add Active Directory data enrichment for user names on page 225](#)

Add Hadoop HBase data enrichment source

Pull HBase identity mapping through a Receiver to enrich events by adding Hadoop HBase as a data enrichment source.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Data Enrichment**.
- 2 On the **Data Enrichment Wizard**, fill in the fields on the **Main** tab, then click the **Source** tab.
- 3 In the **Type** field, select **Hadoop HBase (REST)**, then type the host name, port, and name of the table.
- 4 On the **Query** tab, fill in the lookup column and query information:
 - a Format **Lookup Column** as `columnFamily:columnName`
 - b Populate the query with a scanner filter, where the values are Base64 encoded. For example:

```
<Scanner batch="1024">
<filter>
{
  "type": "SingleColumnValueFilter",
  "op": "EQUAL",
  "family": " ZWlwbG95ZWVJbmZv",
  "qualifier": "dXNlcm5hbWU=",
  "latestVersion": true,
  "comparator": {
    "type": "BinaryComparator",
    "value": "c2NhcGVnb2F0"
  }
}
</filter>
</Scanner>
```

- 5 Complete the information on the **Scoring** and **Destination** tabs.

See also[Data enrichment on page 220](#)[Add data enrichment sources on page 221](#)[Add Hadoop HBase data enrichment source on page 224](#)[Add Hadoop Pig data enrichment source on page 225](#)[Add Active Directory data enrichment for user names on page 225](#)

Add Hadoop Pig data enrichment source

You can leverage Apache Pig query results to enrich Hadoop Pig events.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**.
- 2 Click **Data Enrichment**, then click **Add**.
- 3 On the **Main** tab, fill in the fields, then click the **Source** tab. In the **Type** field, select **Hadoop Pig** and fill in: Namenode host, Namenode port, Jobtracker host, and Jobtracker port.



Jobtracker information is not required. If Jobtracker information is blank, NodeName host and port are used as the default.

- 4 On the **Query** tab, select the **Basic** mode and fill in the following information:
 - a In **Type**, select **text file** and enter the file path in the **Source** field (for example, `/user/default/file.csv`). Or, select **Hive DB** and enter an HCatalog table (for example, `sample_07`).
 - b In **Columns**, indicate how to enrich the column data.

For example, if the text file contains employee information with columns for SSN, name, gender, address, and phone number, enter the following text in the **Columns** field: `emp_Name:2, emp_phone:5`. For Hive DB, use the column names in the HCatalog table.
 - c In **Filter**, you can use any Apache Pig built-in expression to filter data. See Apache Pig documentation.
 - d If you defined column values above, you can group and aggregate that column data. Source and Column information is required. Other fields can be blank. Using aggregation functions require that you specify groups.
- 5 On the **Query** tab, select the **Advanced** mode and enter an Apache Pig script.
- 6 On the **Scoring** tab, set the score for each value returned from the single column query.
- 7 On the **Destination** tab, select the devices to which you want to apply enrichment.

See also

[Data enrichment on page 220](#)

[Add data enrichment sources on page 221](#)

[Add Hadoop HBase data enrichment source on page 224](#)

[Add Active Directory data enrichment for user names on page 225](#)

Add Active Directory data enrichment for user names

You can leverage Microsoft Active Directory to populate Windows events with the full user display names.

Before you begin

Verify that you have the System Management privilege.

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, select **System Properties**.
- 2 Click **Data Enrichment**, then click **Add**.
- 3 On the **Main** tab, enter a descriptive **Enrichment Name**, in the form `Full_Name_From_User_ID`.
- 4 Set both the **Lookup Type** and **Enrichment Type** to **String**.
- 5 Set **Pull Frequency** to **daily**, unless Active Directory is updated more frequently.
- 6 Click **Next** or the **Source** tab.
 - a In the **Type** field, select **LDAP**.
 - b Fill in the IP address, user name, and password.
- 7 Click **Next** or the **Query** tab.
 - a In the **Lookup Attribute** field, enter `sAMAccountName`.
 - b In the **Enrichment Attribute** field, enter `displayName`.
 - c In **Query**, enter `(objectClass=person)` to return a list of all objects in Active Directory classified as a person.
 - d Test the query, which returns a maximum of five values, regardless of the number of actual entries.
- 8 Click **Next** or the **Destination** tab.
 - a Click **Add**.
 - b Select your Microsoft Windows data source.
 - c In the **Lookup Field**, select the **Source User** field.

This field is the value that exists in the event, which is used as the index for the lookup.
 - d Select the **Enrichment Field**, where the enrichment value is written in the form `User_Nickname` or `Contact_Name`.
- 9 Click **Finish** to save.
- 10 After writing the enrichment settings to the devices, click **Run Now** to retrieve the enrichment values from the data source until the **Daily Trigger Time** value occurs.

The **Full Name** is written into the **Contact_name** field.

See also

[Data enrichment on page 220](#)

[Add data enrichment sources on page 221](#)

[Add Hadoop HBase data enrichment source on page 224](#)

[Add Hadoop Pig data enrichment source on page 225](#)

4

Working with dashboard views

Visual, interactive ESM dashboard views enable you to monitor threats to your organization at a glance. The ESM dashboard can contain multiple views and interactive tabs that allow you to move quickly between your views. You can use predefined views or build your own unique views with widgets and filters.

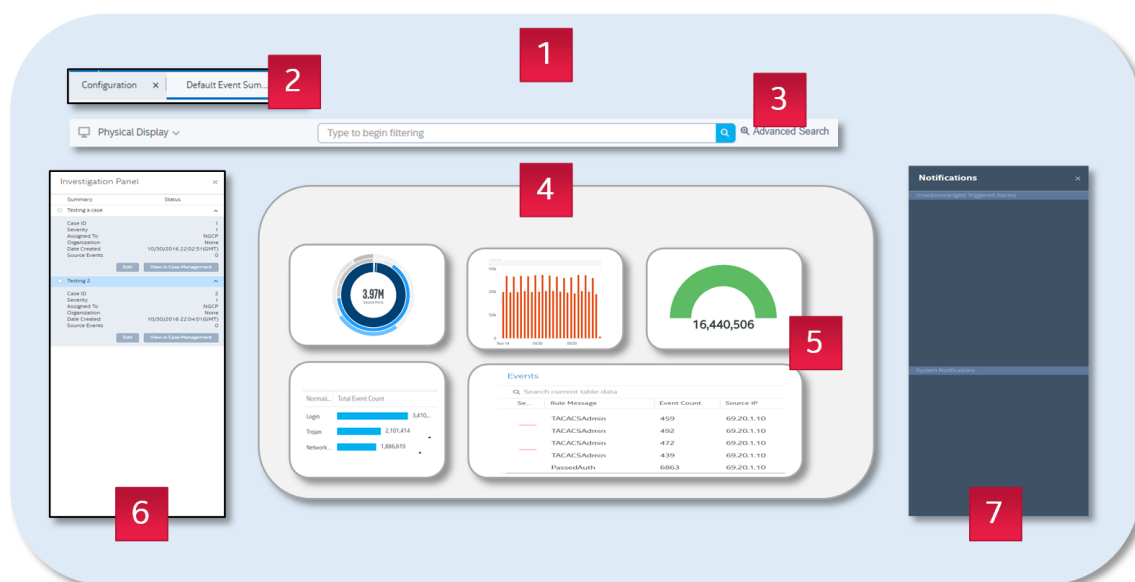
Contents

- ▶ *Dashboard building blocks*
- ▶ *Predefined (default) views*
- ▶ *Open dashboard views*
- ▶ *Add custom dashboard views*
- ▶ *Bind dashboard widgets*
- ▶ *Filter dashboard views*
- ▶ *Respond to notifications*
- ▶ *Investigate open cases*

Dashboard building blocks

Once you learn what makes up a dashboard view, you can build interactive views that enable you to investigate potential threats unique to your organization.

Dashboards are visual tools that you can use to represent data in a form that enables you to see possible threats quickly.



- 1 Populate your ESM dashboard workspace with predefined views or your own custom views.
- 2 Navigate between views quickly using tabs. Use tabs to explore potential threat across multiple views while still retaining the historical context that has initiated the investigation in a separate tab.
- 3 Use the filter ribbon to find what you're looking for in query results using real-time functionality. Autocomplete returns results as you build the filter query.
- 4 Build multiple dashboard views that enable you to pivot, explore, investigate, and respond to potential threats.
- 5 Represent and drill-down to specific data quickly using interactive, visual widgets.
- 6 Investigate open cases without leaving the dashboard, giving you quick access to critical case details.
- 7 Respond to unacknowledged, triggered alarms and system notifications.

Predefined (default) views

The **Default Views** list gives you access to the dashboard views that come with McAfee ESM.

The **Add View** menu on the dashboard contains the following types of default views:

- **Asset, Threat & Risk** views summarize asset, threat, and risk data and their possible effects on your system.
- **Dashboard Views** provide an overview of specific aspects of the system.
- **Device** views show the status of selected devices.
- **Event Views** break down information generated by events associated with selected devices.
- **Flow Views** break down the information recorded about each flow (or connection).

Open dashboard views

You can open, import, or export more than one dashboard view at a time. You can also copy predefined (default) views or create custom views to suit the needs of your organization.

Before you begin

Verify that you have administrator rights or belong to an access group with view management permission.

Task

- 1 On the dashboard, click **Add View** and click the slide-out arrow next to one of the following options.
 - To open an existing view, click **Open View**.
 - To convert a Flash view into an HTML dashboard view, click **Import Flash Views**.
 - To create an HTML view, click **Create New View**. Add widgets and save your view.
- 2 Save your view.






Add custom dashboard views

Create unique dashboard views by adding and arranging widgets that enable you to display and interact with specific information.

Before you begin

Verify that you have administrator rights or belong to an access group with view management permission.

Task

- 1 On the dashboard, click **Add View**.
 - 2 To create an HTML view, click **Create New View**.
 - 3 Click  **Edit**.
 - 4 Click **Add Widget** and do the following:
 - Give your widget a title.
 - From the available options, select a query source, which prepopulates the query fields, filters, and sorting values. You can use the defaults or change the values.
-  The query source you choose determines which visualization options you can choose for the widget.
- Select the widget's visualization option. Possible options include: tables, bar charts, pie charts, gauges, and interactive donut charts.
 - Select whether to bind the widget to data in another widget.
 - 5 Click **Create**. Once the widget appears on your dashboard, you can change its size and placement.
 - 6 To change the widget once it appears on the dashboard view, click . The options on the submenu vary depending on the widget and its corresponding data. Options might include:  **Settings**,  **Visualization**, **Details**, **Actions**, **Drilldown**, **Filter On**, and **Delete**.
 - 7 Click **Save**.

Bind dashboard widgets

Binding dashboard widgets links the data between those widgets. Then, when you change data in a parent widget, the data in the bound widget also changes, creating an interactive view. For example, if you bind a widget to a source IP address and then choose a specific IP address in the parent widget, the bound widget filters its data by that IP address. Changing the selection in the parent widget refreshes the child widget's data.




Before you begin

Verify that you have administrator rights or belong to an access group with view management permission.

Task

- 1 Open or create a dashboard view with the widgets that you want to bind.

 You can bind widgets to one data field only.

- 2 To edit the dashboard view, click  **Edit**.
- 3 On the widget you want to bind, click  . Then, select  **Settings**.
- 4 In the **Widget Configuration** pane, turn on **Binding** and select the data you want to filter on (or link to) the widget.
- 5 Click **Save**.

The  icon appears on bound widgets. Hovering over the icon reveals what data the widget is bound to.

- 6 Click **Save** again to save your change to the dashboard view and exit the **Edit** mode.

See also

[Working with the Query Wizard on page 311](#)

[Manage queries on page 312](#)

[Comparing values on page 314](#)

[Compare graph values on page 314](#)

[Set up stacked distribution for views and reports on page 315](#)

Filter dashboard views


Filter your dashboard view so that you can focus on specific details in the view.


Before you begin



Verify that you belong to an access group with view management or view data permissions.

Task

- 1 Open the dashboard view you want to filter.
- 2 To filter the view, do one of the following:
 - Click the **Filter** bar and add the relevant field and values.

 You can only use the AND operator in the **Filter** bar.

 - Accept the default equals (=) operator in the filter.
 - To change the operator to not equals (!=), click the equals sign (=).
 - To remove a field from the filter, click  on that field.
 - To build complex filters using both AND and OR operators, click **Advanced Search**.
 - To apply predefined filter sets to the view, click the **Filter Sets** drop-down arrow in the top right corner of the dashboard.
 - Select a predefined filter set from the list.
 - To create a filter set, click **Manage Filter Sets**.

 For details about how to create a filter set, click  on the **Managing Filter Sets** window.

- 3 To filter the view, click .

The view refreshes to display only the records matching the values you entered.









Respond to notifications

Respond to triggered alarms from the dashboard. You can also view system notifications.

Before you begin

Verify that you have administrator rights or belong to an access group with alarm management permission.

Task

- 1 To show triggered alarms and system notifications on the dashboard, click .
- 2 Respond to triggered alarms in one of the following ways:
 - Acknowledge triggered alarms by selecting the appropriate alarm and clicking . The system removes acknowledged alarms from the **Notifications** panel. You can still view the alarms on the **Triggered Alarms** view.
 - Delete alarms by selecting the appropriate alarm and clicking .
 - Filter alarms by using the filter bar. Then, to refresh the view, click .
 - Assign alarms by clicking . Then, select the appropriate alarm and click **Assignee** to choose a specific person to respond to the alarm.
 - Create a case for the alarm by clicking . Then, select the appropriate alarm and click **Create Case**.
 - Edit the triggered alarm settings by clicking the appropriate alarm. Click  to change the settings.
 - View details about triggered alarms by clicking . Then, do one of the following:
 - To see what event triggered the alarm, click the **Triggering Event** tab. To view the description, double-click the event.
 - To see what condition triggered the alarm, click the **Condition** tab.
 - To see what actions occurred as a result of the triggered alarm, click the **Action** tab.

Investigate open cases

From the dashboard, you can track work related to open cases.

Before you begin

Verify that you have administrator rights or belong to an access group with case management permission.

Task

- 1 To view open cases from the dashboard, click  and select **Investigation Panel**.

A summary of open cases appears on the left side of the dashboard.

- 2 Use the drop-down arrow to expand the case you want to investigate. Do one of the following:
 - To change the case details (severity, assignee, values, or notes) from the dashboard, click **Edit**. Make your changes and click **Save**.
 - To view the case details, click **View in Case Management**.
- 3 Close the **Investigation Panel**.

5

Managing cyber threats

McAfee ESM allows you to retrieve indicators of compromise (IOC) from remote sources and quickly access related IOC activity in your environment.

Cyber threat management enables you to set up automatic feeds that generate watchlists, alarms, and reports, giving you visibility to actionable data. For example, you can set up a feed that automatically adds suspicious IP addresses to watchlists to monitor future traffic. That feed can generate and send reports indicating past activity. Use **Event Workflow views > Cyber Threat Indicators** views to drill down quickly to specific events and activity in your environment.

Contents

- *Set up cyber threat management*
- *Set up cyber threat feed for domain*
- *View cyber threat feed results*
- *Supported indicator types*
- *Errors on manual upload of an IOC STIX XML file*

Set up cyber threat management

Set up feeds to retrieve indicators of compromise (IOC), STIX formatted XML, from remote sources. You can then use these feeds to generate watchlists, alarms, and reports that allow users to access related IOC activity in your environment.

Before you begin

Verify that you have the following permissions:

- Cyber Threat Management - allows user to set up a cyber threat feed.
- Cyber Threat User - allows user to view the data generated by the feed.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, click **System Properties**.
- 2 Click **Cyber Threat Feeds**, then click **Add**.
- 3 On the **Main** tab, enter the feed name.
- 4 On the **Source** tab, select the source data type and its connection credentials. Click **Connect** to test the connection.



Supported sources include McAfee Advanced Threat Defense and MITRE Threat Information Exchange (TAXII).

- 5 On the **Frequency** tab, identify how often the feed pulls the IOC files (pull frequency). Available pull frequencies include: every x minutes, daily, hourly, weekly, or monthly. Specify the daily trigger time.
- 6 On the **Watchlist** tab, select which property or field in an IOC file to append to an existing watchlist. You can add watchlists for any supported property or field.
If the watchlist you need does not yet exist, click **Create New Watchlist**.
- 7 On the **Backtrace** tab, identify which events (default) and flows to analyze, matching data to analyze, and how far back to analyze data against this feed.
 - a Choose to analyze events, flows, or both.
 - b Indicate how far back (in days) to analyze the events and flows.
 - c Specify what action you want ESM to take if the backtrace finds a data match.
 - d For alarms, select an assignee and severity.
- 8 Return to the **Main** tab, then select **Enabled** to activate this feed.
- 9 Click **Finish**.

You are informed when the process is completed successfully.



New file and indicator validations have been added to the manual upload source type. If you receive an error when you select this source type, see *Errors on manual upload of an IOC STIX XML file* to troubleshoot it.

See also

[View cyber threat feed results on page 235](#)

[Supported indicator types on page 235](#)

[Errors on manual upload of an IOC STIX XML file on page 236](#)

Set up cyber threat feed for domain

To enable a domain feed, you must have two watchlists to hold IP address and domain data.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM system navigation tree, select **System Properties | Cyber threat feeds | Add**, then create a feed (see *Set up cyber threat management*).
- 2 On the **Watchlist** tab, click **Create New Watchlist**, and add two watchlists (see *Add a watchlist*):
 - **Name:** CyberThreatIP, **Type:** IP Address
 - **Name:** CyberThreatDomain, **Type:** Web_Domain
- 3 In the **Indicator Type** field, select **IPv4**, then select CyberThreatIP in the **Watchlist** field.
- 4 In the next **Indicator Type** field, select **Fully Qualified Domain Name**, then select CyberThreatDomain in the **Watchlist** field.
- 5 Complete the cyber threat feed setup, then click **Finish**.


View cyber threat feed results

View indicators of compromise (IOC) from external data sources, identified by your organization's cyber threat feeds. Quickly drill down to the threat details, file descriptions, and corresponding events for each indicator source.

Before you begin

Verify that you have the **Cyber Threat User** permission, which allows you to view the results of your organization's cyber threat feeds.

Task

- 1 From the dashboard, click  and select **Cyber Threat Indicators**.
- 2 On the ESM console, click the view list, then select **Event Workflow Views | Cyber Threat Indicators**.
- 3 On the time frame list, select the time period for the view.
- 4 Filter by feed name or supported IOC data types.
- 5 Perform any standard view action, including:
 - Create or append to a watchlist.
 - Create an alarm.
 - Execute a remote command.
 - Create a case.
 - Look around or last look around.
 - Export the indicator to a CSV or HTML file.
- 6 Drill down to threat details using the **Description**, **Details**, **Source Events**, and **Source Flows** tabs

See also

[Set up cyber threat management on page 233](#)

[Supported indicator types on page 235](#)

[Errors on manual upload of an IOC STIX XML file on page 236](#)

Supported indicator types

When you add a manual upload cyber threat feed, the ESM sends the Structured Threat Information Expression (STIX) file to the Indicator of Compromise (IOC) engine to be processed. If the file doesn't contain an indicator that is normalized for the ESM, you receive an error message.

Table 5-1 Indicator types normalized for ESM

Indicator type	Watchlist type
Email Address	To, From, Bcc, Cc, Mail_ID, Recipient_ID
File Name, File Path	File_Path, Filename, Destination_Filename, Destination_Directory, Directory
(Flows) IPv4, IPv6	IPAddress, Source IP, Destination IP
(Flows) MAC Address	MacAddress, Source MAC, Destination MAC
Fully Qualified Domain Name, Host Name, Domain Name	Host, Destination_Hostname, External_Hostname, Domain, Web_Domain

Table 5-1 Indicator types normalized for ESM *(continued)*

Indicator type	Watchlist type
IPv4, IPv6	IPAddress, Source IP, Destination IP, Attacker_IP, Grid_Master_IP, Device_IP, Victim_IP
MAC Address	MacAddress, Source MAC, Destination MAC
MD5 Hash	File_Hash, Parent_File_Hash
SHA1 Hash	SHA1
Subject	Subject
URL	URL
Username	Source User, Destination User, User_Nickname
Windows Registry Key	Registry_Key, Registry.Key (Registry subtype)
Windows Registry Value	Registry_Value, Registry.Value (Registry subtype)

See also

Set up cyber threat management on page 233

View cyber threat feed results on page 235

Errors on manual upload of an IOC STIX XML file on page 236

Errors on manual upload of an IOC STIX XML file

When you add a manual upload cyber threat feed, the ESM sends the Structured Threat Information Expression (STIX) file to the Indicator of Compromise (IOC) engine to be processed.

If there is a problem with the upload, you receive one of these errors.

Table 5-2 Cyper threat manual upload errors

Error	Description	Troubleshooting
ER328 — Invalid STIX format	The file format is incorrect.	<ul style="list-style-type: none"> Make sure that the uploaded file is a STIX file. The engine supports STIX version 1.1. Read the STIX documentation to verify that the schema is valid. <ul style="list-style-type: none"> Open Standards for Information Society (OASIS) — Organization in charge of STIX standards (https://www.oasis-open.org/). STIX Project — Contains the various STIX data models, schemas, and xsd documents (https://stixproject.github.io/).
ER329 — No supported IOCs found	The uploaded STIX file doesn't contain indicators that are normalized for the ESM.	If a specific indicator needs to be processed, please contact McAfee Support so that it can be normalized for the ESM. See <i>Supported indicator types</i> for a list of indicator types that are supported by ESM.

See also

Set up cyber threat management on page 233

View cyber threat feed results on page 235

Supported indicator types on page 235

6

Working with content packs

When a specific threat situation occurs, respond immediately by importing and installing the relevant content pack from the rules server. Content packs contain use-case driven correlation rules, alarms, views, reports, variables, and watchlists to address specific malware or threat activity. Save time by using content packs instead of developing tools in-house.

[Search the McAfee content pack catalog.](#)

Contents

- [Importing content packs](#)
- [Install content packs](#)
- [Modify content packs](#)

Importing content packs

Content packs are typically downloaded as part of automatic rules updates. If your ESM does not automatically download rules and content packs, use this manual process.

Before you begin

Verify that you have the following permissions:

- System Management
- User Administration

Task

- 1 [Go to McAfee Connect.](#)
- 2 Browse the available content packs and download the one you want.
- 3 Install the content pack on the ESM.

Install content packs

Select a content pack and deploy it.

Task

- 1 From the main ESM dashboard, click the **System Properties** icon.
- 2 Click **Content Packs**.
- 3 Click **Browse**.

The Browse Content Packs window opens.

- 4 Browse the list and select the content pack you want.



Clicking a name or description shows the details for that content pack. Clicking the check box selects the content pack for installation.

- 5 Click **Install**.
- 6 Complete any post-installation steps listed in the details of the content pack.

Modify content packs

Update or uninstall a content pack.



If you have customized content pack elements, the update process might overwrite the customized elements.

Task

- 1 From the ESM configuration dashboard, click the **System Properties** icon.
- 2 Click **Content Packs**.
The list of installed content packs appears.
- 3 Browse the list for available updates.
If a newer version of the content pack is available, the status will read **Update Available**.
- 4 To update a content pack, select it and then click **Update**.
- 5 To uninstall a content pack, select it and then click **Uninstall**.

7

Alarms workflow

Familiarize yourself with the alarms workflow. Click the relevant task link for detailed step-by-step information.

Contents

- [Prepare to build alarms](#)
- [Build alarms](#)
- [Monitor and respond to alarms](#)
- [Tune alarms](#)

Prepare to build alarms

Before you can build and respond to alarms, ensure that your ESM environment contains the following building blocks: alarm message templates, message recipient groups, mail server connection, alarm audio files, alarm reports queue, and visible alarms tab on the dashboard.

Before you begin

To view triggered alarms on the dashboard, see [Select user settings](#) on page 193.

Read through the following tasks to learn how to prepare your alarms environment.

Tasks

- [Set up alarm messages on page 239](#)
Configure ESM to send triggered alarm messages, using email, Short Message Services (SMS), Simple Network Management Protocol (SNMP), or syslog.
- [Manage alarm audio files on page 244](#)
Upload and download audio files to use with alarm alerts.

Set up alarm messages

Configure ESM to send triggered alarm messages, using email, Short Message Services (SMS), Simple Network Management Protocol (SNMP), or syslog.

Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

Tasks

- [Create alarm message templates on page 240](#)
Create alarm message templates for email, Short Message Services (SMS), Simple Network Management Protocol (SNMP), or syslog. You can then associate the templates with specific alarm actions and message recipients.
- [Set up correlation alarms to include source events on page 241](#)
To include source events information in alarm results, set up an **Internal Event Match** or **Field Match** alarm that uses a correlation event as the match.
- [Manage alarm recipients on page 243](#)
Identify alarm message recipients and configure how to send those alarm messages, using email, Short Message Services (SMS), Simple Network Management Protocol (SNMP), or syslog.

Create alarm message templates


Create alarm message templates for email, Short Message Services (SMS), Simple Network Management Protocol (SNMP), or syslog. You can then associate the templates with specific alarm actions and message recipients.


Before you begin


Verify that you have administrator rights or belong to an access group with alarm management privileges.


For details about product features, usage, and best practices, click **?** or **Help**.



Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**.
- 3 Click the **Settings** tab, then click **Templates**.
 - To create custom templates, click **Add**.
 - To change a custom template, select it and click **Edit**.

 You cannot edit predefined templates.
 - To delete a custom template, select it and click **Remove**.

 You cannot delete predefined templates.
 - To copy an existing template, select it and click **Copy**. Save the copied template with a new name.
 - To set a default for all alarm messages, select it and click **Make Default**.
- 4 On the **Template Management** page, add or change the following information.

Option	Description
Type	Select whether this template is for an email message or SMS message. <div data-bbox="500 1759 1520 1829">  SMS messages are sent as email to a phone and converted to SMS by the carrier. SMS messages are limited to 140 characters. </div>
Name	Type the name for this template.
Description	Type a description of what this template includes.

Option	Description
Make Default	Use the current template as the default when sending messages.
Subject	For an email template, select the subject for the message. Click the Insert Field icon and select the information that you want to include in the subject line of the message.
Message Body	<p>Select the fields that you want to include in the body of the message.</p> <div>  <p>For syslog message templates, limit the message body to fewer than 950 bytes. ESM cannot send any syslog message that exceeds 950 bytes.</p> </div> <ul style="list-style-type: none"> • Delete either of the fields included by default if you don't want them included in the message. • Position the cursor in the body where you want to insert a data field. Click the Insert Field icon above the Subject field. Then select the type of information you want this field to display. • If you select Repeating Block, ESM adds the syntax required to loop through records. Insert the fields that you want to include for each record between the [\$REPEAT_START] and [\$REPEAT_END] markers. ESM then includes this information in the message for up to 10 records. • Set up correlation alarms to include source events on page 241 To include source events in alarms that use a correlation event as a match (), click the Insert Field icon and select Source Events Block. <div>  <p>When you select Internal Event Match or Field Match as the alarm type, ESM includes event field data in the email. Select Field Match for data source-driven alarms, which run on the Receiver not the ESM. Select Internal Event Match alarms, which run on the ESM and force a query to run every time the alarm frequency expires.</p> </div>

See also

[Defining message settings](#) on page 156

[Set up correlation alarms to include source events](#) on page 241

[Manage alarm recipients](#) on page 243

Set up correlation alarms to include source events


To include source events information in alarm results, set up an **Internal Event Match** or **Field Match** alarm that uses a correlation event as the match.


Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

For details about product features, usage, and best practices, click **?** or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**.
- 3 Click the **Settings** tab, then click **Templates**.
- 4 On the **Template Management** page, click **Add**, then enter the information requested.

- 5 In the **Message Body** section, place your cursor where you want to insert the tags, then click the **Insert Field** icon , and select **Source Event Block**.
- 6 Place your cursor inside the tags, click the **Insert Field** icon again, then select the information you want to include when the correlation alarm triggers.

The following example shows what an alarm message template looks like when you insert fields for an event's source IP address, destination IP address, and severity:

```
Alarm: [$Alarm Name]
Assignee: [$Alarm Assignee]
Trigger Date: [$Trigger Date]

Summary: [$Alarm Summary]

[$REPEAT_START]
Correlation SigID: [$Signature ID]
Correlated Last Time: [$Last Time]

[$SOURCE_EVENTS_START]
Source Event Details:

Last Time: [$Last Time]
SigID: [$Signature ID]
Rule Message: [$Rule Message]
Severity: [$Average Severity]

Src User: [%UserIDSrc]
Src IP: [$Source IP]
Src Port: [$Source Port]

Dst User: [%UserIDDst]
Dst IP: [$Destination IP]
Dst Port: [$Destination Port]

Host: [%HostID]
Command: [%CommandID]
Application: [%AppID]
Packet: [$Packet Data]

[$SOURCE_EVENTS_END]
[$REPEAT_END]
```



If a correlated event does not trigger the alarm, the message does not include the data.

See also

[Defining message settings on page 156](#)

[Create alarm message templates on page 240](#)

[Manage alarm recipients on page 243](#)

Manage alarm recipients


Identify alarm message recipients and configure how to send those alarm messages, using email, Short Message Services (SMS), Simple Network Management Protocol (SNMP), or syslog.

Before you begin

- Verify that you have administrator rights or belong to an access group with alarm management privileges.
- Verify that the profiles you intend to use exist. See [SNMP configuration](#) on page 179 and [Configure profiles](#) on page 177.

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**.
- 3 Click the **Settings** tab, then click **Recipients**.
 - Click **Email** to view or update email addresses for individual recipients.
 - Click **Users** to view user names and email addresses.
 - Click **SMS** to view or update SMS recipients and their addresses.
 - Click **SNMP** to view or update the following SNMP information:

Option	Description
Profile	Select an existing SNMP recipient profile from the drop-down list. To add a profile, click Profile .
Specific Trap Type	Select the specific trap type. The general trap type is always set to 6, Enterprise Specific.
Enterprise OID	Enter the full enterprise object identifier (OID) for the trap to be sent. Include everything from the first 1 through the enterprise number, including any subtrees within the enterprise.
Contents	Include Informative Data Bindings — The trap contains variable bindings information, including the line number of the processed report, string identifying the trap source, name of the notification generating the trap, and ID of the ESM sending the trap. Include report data only — The extra variable bindings are not included in the trap.

Option	Description
Formatting	Each SNMP trap generated from a report contains one line of data from that report. <ul style="list-style-type: none"> • Send each report line as is — The data from the report line is sent as is in a single variable binding. The system constructs the data binding OIDs by concatenating the Enterprise OID, the specific trap type, and an auto-incrementing number beginning with the number 1. • Parse results and use these binding OIDs — The system parses the report line and sends each field in a separate data binding.
Binding OID List	Parse results and use these binding OIDs — Specify custom data binding OIDs. <ul style="list-style-type: none"> • If you select this option, click Add and type the binding OID value. • If you do not specify variable OIDs for all data fields in the report, ESM begins incrementing from the last OID specified in the list.

- 4 Click **Syslog** to view or update the following syslog information:

Option	Description
Host IP and Port	Enter each recipient's host IP address and port.
Facility and Severity	Select the facility and the severity of the message.

See also

[Defining message settings on page 156](#)

[Create alarm message templates on page 240](#)

[Set up correlation alarms to include source events on page 241](#)

Manage alarm audio files


Upload and download audio files to use with alarm alerts.

Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

For details about product features, usage, and best practices, click **?** or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click the **Settings** tab, then click **Audio**.
- 3 Download, upload, remove, or play audio files, then click **Close**.



ESM includes three pre-installed sound files. You can upload custom audio files.

Build alarms

Alarms drive actions in response to specific threat events. Building too many or too few alarms that trigger frequently can create distracting noise. The best approach is to build alarms that escalate events that are critical to your organization.

With McAfee ESM you can build alarms: enabling pre-built alarms, copying existing alarms and changing them, or creating alarms specific to your organization.

Read the following tasks to learn more about how to build alarms.

Tasks

- [Enable or disable alarm monitoring on page 245](#)
Toggle alarm monitoring on or off for the entire system or for individual alarms. ESM alarm monitoring is turned on (enabled) by default.
- [Copy an alarm on page 245](#)
Use an existing alarm as a template for a new alarm by copying and saving it with a different name.
- [Create alarms on page 246](#)
Create an alarm so that it triggers when your defined conditions are met.

Enable or disable alarm monitoring

Toggle alarm monitoring on or off for the entire system or for individual alarms. ESM alarm monitoring is turned on (enabled) by default.

Before you begin


Verify that you have administrator rights or belong to an access group with alarm management privileges.



If you disable alarm monitoring for the system, ESM generates no alarms.

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**.
- 3 To disable or enable alarm monitoring for the entire system, click the **Settings** tab, then click **Disable** or **Enable**.
- 4 To disable or enable individual alarms, click the **Alarms** tab. The **Status** column indicates whether alarms are *enabled* or *disabled*.
 - To enable (turn on) a specific alarm, highlight it and select **Enabled**.
 - To disable (turn off) a specific alarm, highlight it and deselect **Enabled**. ESM no longer generates this alarm.
- 5 Click **OK**.

See also

[Copy an alarm on page 245](#)

[Create alarms on page 246](#)

Copy an alarm


Use an existing alarm as a template for a new alarm by copying and saving it with a different name.

Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**.
- 3 Select an enabled alarm, then click **Copy**.

The **Alarm Name** page displays the name of the current alarm followed by `_copy`.



You can copy only enabled alarms. Disabled alarms cannot be copied.

- 4 Change the name, then click **OK**.
- 5 To make changes to the alarm settings, select the copied alarm and click **Edit**.
- 6 Change the settings as needed.

See also

[Enable or disable alarm monitoring on page 245](#)

[Create alarms on page 246](#)

Create alarms


Create an alarm so that it triggers when your defined conditions are met.


Before you begin



Verify that you have administrator rights or belong to an access group with alarm management privileges.

For details about product features, usage, and best practices, click ? or **Help**.

Task



- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**, then click **Add**.
- 3 Click the **Summary** tab to define the general alarm settings.
 - Name the alarm.
 - From the **Assignee** list, select the person or group to assign this alarm to. This list includes all users and groups with the **Alarm Management** privilege.
 - In **Severity**, select the alarm's priority in the alarm log (high is 66–100, medium is 33–65, low is 1–32).
 - Select **Enabled** to turn on this alarm and deselect the box to turn off the alarm.
- 4 On the **Condition** tab, identify which conditions trigger the alarm.







Condition	Description
Check Rate	Select how often the system checks for this condition.
Deviation	<p>Specify a percentage threshold to check above baseline and a different percentage below baseline.</p> <ul style="list-style-type: none"> • Query — Select the type of data you are querying. • Filters icon — Select the values to filter the data for this alarm. • Time Frame — Select whether to query the last or previous time period selected in the number field. • Trigger when the value is — Select how far above and below the baseline the deviation is before ESM triggers the alarm.
Event Rate	<ul style="list-style-type: none"> • Event Count — Enter the number of events that must occur before ESM triggers the alarm. • Filters icon — Select the values to filter the data. • Time Frame — Select in what interval the number of selected events must occur before ESM triggers the alarm. • Offset — Select how long to offset so the alarm does not include the sharp increase at the end created by aggregation. For example, if ESM pulls events every five minutes, the last one minute of the events retrieved contain the aggregated events. Offset the time period by that amount so the last one minute is not included in the data measurement. Otherwise, ESM includes the values in the aggregated data in the event count, causing a false positive.
Field Match	<ol style="list-style-type: none"> 1 Drag and drop the AND or OR icon to set up the logic for the alarm's condition. 2 Drag and drop the Match Component icon onto the logic element, then complete the Add Filter Field page. 3 Limit the number of notifications you receive by setting the Maximum Condition Trigger Frequency. Each trigger only contains the first source event that matches the trigger condition, not the events that occurred within the trigger frequency period. New events that match the trigger condition do not cause the alarm to trigger again until after the maximum trigger frequency period. For example, if you set the frequency to 10 minutes and an alarm triggers five times within a 10-minute period, ESM sends a single notice containing 5 alarms. <div>  If you set the interval to zero, every event that matches a condition triggers an alarm. For high frequency alarms, a zero interval can produce many alarms. </div>
Health Monitor Status	Select the types of device status changes. For example, if you select only Critical , you are not notified if there is a health monitor status change at the Warning level.


Condition	Description
Internal Event Match	<ul style="list-style-type: none"> • Trigger when value does not match — Select to trigger the alarm when the value doesn't match your setting. • Use Watchlist — Select if a watchlist contains the values for this alarm. <ul style="list-style-type: none">  Values containing commas must be in a watchlist or in quotes. • Field — Select the type of data this alarm monitors. <ul style="list-style-type: none">  For alarms that trigger when a health monitor event is generated. • Value(s) — Type the specific values of the type selected in Field (limited to 1,000 characters). For example, for Source IP, enter the actual source IP addresses that trigger this alarm.
Maximum Condition Trigger Frequency	Select the amount of time to allow between each condition to prevent a flood of notifications.
Threshold	Event Delta condition type only — Select the maximum allowed delta for the analyzed events before the alarm triggers.
Type	Select the alarm type, which determines the fields you must fill in.

5 On the **Devices** tab, select which devices this alarm monitors.

6 On the **Actions** tab, identify what happens when the alarm triggers.

Action	Description
Log event	Create an event on the ESM.
Auto-acknowledge Alarm	Acknowledge the alarm automatically, right after it triggers. As a result, the alarm doesn't appear on the Alarms pane but the system adds it to the Triggered Alarms view.
Visual alert	Generate an alarm notification on the bottom right of the console. To include an audio notification, click Configure --> Play Sound , then select an audio file.
Create case	<p>Create a case for the selected person or group. Click Configure to identify the case owner and to select which fields to include in the case summary.</p> <ul style="list-style-type: none">  If you plan to escalate alarms, do not create cases.
Update watchlist	<p>Change watchlists by adding or removing values based on the information contained in up to 10 alarm-triggering events. Click Configure and select which field from the triggering event to append to or remove from the selected watchlist. When these settings change a watchlist, the Actions tab on the Triggered Alarm view shows the change.</p> <ul style="list-style-type: none">  This action requires Internal Event Match as the condition type.

Action	Description
Send message	<p>Send an email or SMS message to the selected recipients.</p> <ul style="list-style-type: none"> Click Add recipient, then select the message recipients. Click Configure to select the template (for email, SMS, SNMP, or syslog messages) and the time zone and date format to use for the message. <p> Using the following characters in alarm names might cause issues when sending SMS messages: comma (,), quotation marks ("), parenthesis (), forward or backward slash (/ \), semicolon (;), question mark (?), at symbol (@), brackets ([]), more than and less than signs (< >), and equal sign (=).</p>
Generate reports	<p>Generate a report, view, or query. Click Configure, then select a report on the Report Configuration page or click Add to design a new report.</p> <p> If you plan to email a report as an attachment, check with your mail administrator to determine the maximum size for attachments. Large email attachments can prevent a report from being sent.</p>
Execute remote command	<p>Execute a remote command on any device that accepts SSH connections, except McAfee devices on the ESM. Click Configure to select the command type and profile; time zone and date format; and the host, port, user name password, and command string for the SSH connection.</p> <p> If the alarm condition is Internal Event Match, you can track specific events. Click the Insert variable icon  and select the variables.</p>
Send to Remedy	<p>Send up to 10 events to Remedy per triggered alarm. Click Configure to set up the information required to communicate with Remedy: from and to data, prefix, keyword, and user ID (EUID). When events are sent to Remedy, ESM adds Sent events to Remedy to the Actions tab on the Triggered Alarm view. This action requires Internal Event Match as the condition type.</p>
Assign Tag with ePO	<p>Apply McAfee ePolicy Orchestrator tags to the IP addresses that trigger this alarm. Click Configure and select the following information:</p> <ul style="list-style-type: none"> Select ePO device — Device to use for tagging Name — Tags you want applied (only tags available on the selected device appear on the list). Select the field — Field to base the tagging on. Wake up client — Apply the tags immediately. <p> This action requires Internal Event Match as the condition type.</p>
Real Time for ePO Actions	<p>Perform actions from McAfee Real Time for McAfee ePO on the selected McAfee ePO device.</p> <p> This option requires the McAfee Real Time for McAfee ePO plug-in (version 2.0.0.235 or later) and that the McAfee ePO server recognizes that device as one of its endpoints.</p>

Action	Description
Blacklist	<p>Select which IP addresses to blacklist when an alarm triggers. Click Configure and select the following information:</p> <ul style="list-style-type: none"> • Field — Select the type of IP address to blacklist. IP address blacklists both source and destination IP addresses. • Device — Select the device where you want the IP addresses blacklisted. Global adds the device to the Global Blacklist. • Duration — Select how long to blacklist the IP addresses. <p> This action requires Internal Event Match as the condition type.</p>
Custom alarm summary	Customize the fields that are included in the summary of a Field Match or Internal Event Match alarm.

- 7 On the **Escalation** tab, identify how to escalate the alarm when it is unacknowledged within a certain time.

Escalation	Description
Escalate after	Enter the time when you want the alarm to be escalated.
Escalated assignee	Select the person or group to receive the escalated notification.
Escalated severity	Select the severity for the alarm when escalated.
Log event	Select whether to log this escalation as an event.
Visual alert	Select whether the notification is a visual alert. Click Play sound , then select a file if you want a sound to accompany the visual notification.
Send message	Select whether to send the assignee a message. Click Add recipient , select the type of message, then select the recipient.
Generate reports	Select whether to generate a report. Click Configure to select the report.
Execute remote command	Select whether to execute a script on any device that accepts SSH connections. Click Configure , then fill in the host, port, user name, password, and command string.

See also

[Enable or disable alarm monitoring on page 245](#)




[Copy an alarm on page 245](#)

Monitor and respond to alarms

View, acknowledge, and delete triggered alarms using dashboard views, alarm details, filters, and reports.

Read through the following tasks to learn how to monitor and respond to triggered alarms.

- **Viewing triggered alarms** — The **Alarms** log pane on the dashboard lists the total number of alarms by severity.

Symbol	Severity	Range
	High	66–100
	Medium	33–65
	Low	1–32

- **Acknowledging triggered alarms** — The system removes it from the **Alarms** pane. Acknowledged alarms remain on the Triggered Alarms view.
- **Deleting triggered alarms** — The system removes it from the **Alarms** pane and the **Triggered Alarms** view.



If you use visual alerts and do not close, acknowledge, delete a triggered alarm, the visual alert closes after 30 seconds. Audio alerts play until you close, acknowledge, or delete the triggered alarm or click the audio icon to stop the alert.

Tasks

- [View and manage triggered alarms on page 251](#)
View and respond to triggered alarms not yet deleted.
- [Manage alarm reports queue on page 252](#)
If an alarm's action generates reports, you can view the queue of generated reports and cancel one or more of them.

View and manage triggered alarms

View and respond to triggered alarms not yet deleted.

Before you begin

- Verify that you have administrator rights or belong to an access group with alarm management permission.
- Verify with your administrator whether your console is set up to display the **Alarms** log pane.





Task

- 1 Access triggered alarms from one of the following ESM locations:

- On the dashboard, click .
- To view the **Alarms** pane on the console, click and select **Alarms**.
- When an alarm triggers, a pop-up alert opens.

- 2 Do one of the following:

To...	Do this...
Acknowledge an alarm	<ul style="list-style-type: none"> • To acknowledge one alarm, click the checkbox in the first column of the triggered alarm that you want to acknowledge. • To acknowledge several, highlight the items, then click . <p>The system removes acknowledged alarms from the Alarms pane but the alarms remain on the Triggered Alarms view.</p>
Delete an alarm	<ul style="list-style-type: none"> • Select the triggered alarm that you want to delete, then click .
Filter the alarms	<ul style="list-style-type: none"> • Enter the information that you want to use as the filter in the Filters pane, then click .
Change the assignee for alarms	<ol style="list-style-type: none"> 1 To display alarm details, click . 2 Select the alarms, then click Assignee and select the new assignee.

To...	Do this...
Create a case for alarms	<ol style="list-style-type: none"> 1 To display alarm details, click . 2 Select the alarms, then click Create Case and make the selections you need.
View details about an alarm	<ol style="list-style-type: none"> 1 To display alarm details, click . 2 Select the alarm and do one of the following: <ul style="list-style-type: none"> • To view the event that triggered the selected alarm, click the Triggering Event tab. To view a description, double-click the event. <div data-bbox="646 562 690 604" style="display: inline-block; vertical-align: middle;"></div> <div data-bbox="711 556 1461 613" style="display: inline-block; vertical-align: middle; background-color: #f0f0f0; padding: 5px;"> If a single event does not meet the alarm conditions, the Triggering Event tab might not appear. </div> <ul style="list-style-type: none"> • Click the Condition tab to see the condition that triggered the event. • Click the Action tab to see the actions that occurred as a result of the alarm and the ePolicy Orchestrator tags assigned to the event.
Edit triggered alarm settings	<ol style="list-style-type: none"> 1 Click the triggered alarm, then click . Select Edit Alarm. 2 On the Alarm Settings page, make the changes, then click Finish.

See also

[Manage alarm reports queue on page 252](#)

Manage alarm reports queue


If an alarm's action generates reports, you can view the queue of generated reports and cancel one or more of them.

Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

For details about product features, usage, and best practices, click **?** or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**.
- 3 Click the **Settings** tab.
- 4 To view the alarm reports waiting to run, click **View**. ESM runs a maximum of five reports concurrently.
 - View the reports generated by alarms.
 - To stop a specific report from running, select it and click **Cancel**. The remaining reports move up the queue.



If you are an administrator or master user, this list includes all reports waiting to run on the ESM, allowing you to cancel any of them.

- 5 Click **Files** to select whether to download, upload, remove, or refresh any reports on the list.
- 6 Click **Close**.

Table 7-1 Option definitions

Option	Definition
Table	View the reports generated by the ESM that are waiting to run.
Cancel	Click to keep the selected reports from running. The selected reports are cancelled and the remaining reports move up in the queue.

Table 7-2 Option definitions

Option	Definition
Table	View a list of the report files that were generated.
Download	Save the reports you select to another location.
Upload	Add a report to the list.
Remove	Delete a report from the list.
Refresh	Refresh the list to reflect any changes that were made.

See also

[View and manage triggered alarms on page 251](#)

[View Reports page on page 253](#)

View Reports page

View the queue of reports that were generated and are currently running or waiting to run.

Table 7-3 Option definitions

Option	Definition
Table	View the reports generated by the ESM that are waiting to run.
Cancel	Click to keep the selected reports from running. The selected reports are cancelled and the remaining reports move up in the queue.

See also

[Manage alarm reports queue on page 252](#)

Tune alarms

Refine and tune your alarms as you learn what works best for your organization.

Read the following tasks to learn more about how to tune your alarms. These tasks describe how to create specific types of alarms.

Tasks

- [Create UCAPL alarms on page 254](#)
Create alarms that meet Unified Capabilities Approved Products List (UCAPL) requirements.
- [Add health monitor event alarms on page 256](#)
Create alarms based on health monitor events, which can then generate a **Health Monitor Event Summary** report.
- [Add a Field Match alarm on page 263](#)
A **Field Match** alarm matches on multiple fields of an event and triggers when the device receives and parses the event.
- [Customize summary for triggered alarms and cases on page 265](#)
Select the data to include in the alarm summary and the case summary of **Field Match** and **Internal Event Match** alarms.
- [Add an alarm to rules on page 265](#)
To be notified when events are generated by specific rules, you can add an alarm to those rules.
- [Create SNMP traps as alarm actions on page 266](#)
Send SNMP traps as an alarm action.
- [Add a power failure notification alarm on page 266](#)
Add an alarm to notify you when either of the ESM power supplies fail.
- [Manage out-of-sync data sources on page 267](#)
Set up an alarm to alert you when out-of-sync data sources generate events so that you can view a list of data sources, edit their settings, and export the list.

Create UCAPL alarms

Create alarms that meet Unified Capabilities Approved Products List (UCAPL) requirements.

Before you begin


- Verify that you have administrator rights or belong to an access group with alarm management privileges.
- Review the steps to [Create alarms on page 246](#)

For details about product features, usage, and best practices, click **?** or **Help**.

Task

- Set up the alarm types that apply:

Alarm type	Description
Adjustable threshold for failed logons reached	<p>Trigger alarm when multiple failed logons for the same user reach an adjustable threshold.</p> <ol style="list-style-type: none"> 1 Create an Internal Event Match alarm matching on Signature ID. 2 Enter a value of 306–36.
Threshold for no activity reached	<p>Trigger an alarm when a user account is locked due to reaching the no-activity threshold.</p> <ol style="list-style-type: none"> 1 Create an Internal Event Match alarm matching on Signature ID. 2 Enter a value of 306–35.

Alarm type	Description
Allowed concurrent sessions reached	<p>Trigger an alarm if a user attempts to log on to the system after reaching the number of allowed concurrent sessions.</p> <ol style="list-style-type: none"> 1 Create an Internal Event Match alarm matching on Signature ID. 2 Enter a value of 306–37.
Failed system file integrity check	<p>Trigger an alarm when a system file integrity check fails.</p> <ol style="list-style-type: none"> 1 Create an Internal Event Match alarm matching on Signature ID. 2 Enter a value of 306–50085.
Certificates are about to expire	<p>Trigger an alarm when common access card (CAC) or web server certificates are about to expire.</p> <ol style="list-style-type: none"> 1 Create an Internal Event Match alarm matching on Signature ID. 2 Enter a value of 306–50081, 306–50082, 306–50083, 306–50084. <div>  <p>The alarm triggers 60 days before the certificate expires, then on a weekly basis. You cannot change the number of days.</p> </div>
SNMP trap sent when system state not approved	<p>Configure an SNMP trap so that the alarm sends a trap to the NMS when it detects that the system is no longer operating in an approved or secure state.</p> <ol style="list-style-type: none"> 1 Create an alarm matching on any condition, then go to the Actions tab and select Send Message. 2 Click Add Recipients SNMP, select the recipient, then click OK. 3 In the Send Message field, click Configure, click Templates, then click Add. 4 Select SNMP Template in the Type field, enter the text for the message, then click OK. 5 On the Template Management page, select the new template, then click OK. 6 Complete the remaining alarm settings.
Syslog message sent when system state not approved	<p>Configure a syslog message so that the alarm sends a syslog message to NMS when it detects that the system is no longer operating in an approved or secure state.</p> <ol style="list-style-type: none"> 1 Create an alarm matching on any condition, go to the Actions tab, then select Send Message. 2 Click Add Recipients Syslog, select the recipient, then click OK. 3 In the Send Message field, click Configure, then click Templates, and click Add. 4 Select Syslog Template in the Type field, enter the text for the message, then click OK. 5 On the Template Management page, select the new template, then click OK. 6 Complete the remaining alarm settings.
Security log fails to record required events	<p>Configure an SNMP trap so that the alarm notifies the appropriate Network Operations Center (NOC) within 30 seconds if a security log fails to record required events.</p> <ol style="list-style-type: none"> 1 Go to System Properties SNMP Configuration SNMP Traps or device Properties device Configuration SNMP. 2 Select the security log failure trap, then configure one or more profiles for the traps to be sent to, then click Apply. <p>ESM sends SNMP traps to the SNMP profile recipient with the message Failed to write to the security log.</p>

Alarm type	Description
Audit functions start or shut down	Configure an SNMP trap so that the alarm notifies when the audit functions (such as the database, cpservice, IPSDBServer) start or shut down, access SNMP traps or SNMP Settings , and select Database Up/Down Traps . Configure one or more profiles for the traps to be sent to, and click Apply .
Session exists for each administrative role	<p>Trigger an alarm when an administrative session exists for each of the defined administrative roles.</p> <ol style="list-style-type: none"> 1 Create an Internal Event Match alarm matching on Signature ID. 2 Enter the values 306–38 for Audit Administrator, 306–39 for Crypto-Administrator, and 306–40 for Power User. You can also set up separate alarms.



Add health monitor event alarms

Create alarms based on health monitor events, which can then generate a **Health Monitor Event Summary** report.

Before you begin

- Verify that you have administrator rights or belong to an access group with alarm management privileges.
- Review available [Health monitor signature IDs](#) on page 257.
- Review the steps to [Create alarms](#) on page 246.

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 To set up an alarm before a health monitor event is generated:
 - a Set up an alarm **Condition** with the **Internal Event Match** type.
 - b On the **Field** line, select **Signature ID**.
 - c In the **Values** field, enter the signature ID for the health monitor rules.
 - d Fill out the remaining settings for the alarm.
- 2 To set up an alarm if a health monitor event exists:
 - a On the system navigation tree, click the base device for the system  (Local ESM), then select a view that displays the health monitor event (**Event Analysis** or **Default Summary**).
 - b Click the event, then click the **Menu** icon .
 - c Select **Actions** | **Create new alarm from**, then click **Signature ID**.
 - d Fill out the remaining settings for the alarm.

See also

[Health monitor signature IDs](#) on page 257

Health monitor signature IDs

Use these rules to create an alarm that notifies when a health monitor rule event is generated. This list describes the health monitor rules and their signature IDs, type, device, and severity.

Rule name	Signature ID	Description	Type	Device	Severity
A physical network interface connection has been made or removed	306-50080	Network interface settings changed, via an SSH session.	Software Monitor	ESM	Medium
A RAID error has occurred	306-50054	RAID errors encountered.	Hardware Monitor	All	High
Account disabled due to inactivity	306-35	User account disabled, due to inactivity.	Software Monitor	ESM	Medium
Account disabled due to max logon failures	306-36	User account disabled, due to maximum logon failures.	Software Monitor	ESM	High
Add/Edit Remote Command	306-60	Alarm remote command added or deleted.	Software Monitor	ESM	Low
Advanced Syslog Parser collector state change alert	306-50029	ASP parser stopped or started.	Software Monitor	Receiver	Medium
ADM distiller process	306-50066	ADM PDF/DOC text extraction engine stopped or started.	Software Monitor	ADM	Medium
Approved configuration mismatch	146-7	Network discovery device change approved.	Software Monitor	ESM	Low
Archive configuration change	306-3	ESM archival settings changed.	Software Monitor	ESM	Low
Archive process state change alert	306-50051	Receiver archiving process stopped or started.	Software Monitor	ADM/REC/DBM	Medium
Asset vulnerable to event	146-10, 306-10	Vulnerability event created.	Software Monitor	ESM	Low
Audit administrator user logon	306-38	UCAPL event, audit administrator logon.	Software Monitor	ESM	Low
Backup configuration change	306-1	ESM backup configuration settings changed.	Software Monitor	ESM	Low
Backup performed	306-2	Backup performed on the system.	Software Monitor	ESM	Low
Blue Martini parser alert	306-50071	Blue Martini parser stopped or started.	Software Monitor	Receiver	Medium
Bypass NIC state alert	306-50001	NIC entered or exited bypass status.	Software Monitor	IPA/ADM	Medium
CAC cert has expired	306-50082	ESM CAC certificate expired.	Software Monitor	ESM	High
CAC cert expires soon	306-50081	ESM CAC certificate expires soon.	Software Monitor	ESM	Medium
Case changed	306-70	Case changed.	Software Monitor	ESM	Low
Case status added/modified/deleted	306-73	Case status changed.	Software Monitor	ESM	Low
Communication channel state change alert	306-50013	Control channel stopped or started.	Software Monitor	All	Medium

Rule name	Signature ID	Description	Type	Device	Severity
Configuration capture failed (device error)	146-4	Network discovery device error.	Software Monitor	ESM	Low
Configuration capture failed (device unreachable)	146-3	Network discovery device unreachable.	Software Monitor	ESM	Low
Configuration captured	146-5	Network discovery configuration checked successfully.	Software Monitor	ESM	Low
Configuration policy failure	146-8	Not used in system.	Software Monitor	ESM	Low
Configuration policy pass	146-9	Not used in system.	Software Monitor	ESM	Low
Data allocation configuration change	306-7	ESM data allocation settings changed.	Software Monitor	ESM	High
Data partitions free disk space alert	306-50005	Free space on each partition is low (for example, hada_hd has 10% free space).	Software Monitor	All	Medium
Data retention configuration change	306-6	ESM data retention configuration changed.	Software Monitor	ESM	High
Database detection services state alert	306-50036	DBM auto detection service stopped or started.	Software Monitor	All	Medium
Deep packet inspector state change alert	306-50008	Deep packet inspection engine on ADM stopped or started.	Software Monitor	All	Medium
Delete remote command	306-61	Alarm remote command removed.	Software Monitor	ESM	Low
Deleted events	306-74	User deleted ESM events.	Software Monitor	ESM	Low
Deleted flows	306-75	User deleted ESM flows.	Software Monitor	ESM	Low
Device add	306-18	New device added to the system.	Software Monitor	ESM	Low
Device delete	306-19	Existing device deleted from the system.	Software Monitor	ESM	Low
Device possibly down	146-2	Network discovery event stating a device can be down.	Software Monitor	ESM	Low
Device unreachable	146-1	Network discovery device added to ESM is unreachable.	Software Monitor	ESM	Low
Disk drive failure alert	306-50018	Checks and verifies integrity of all hard disks (internal or DAS).	Hardware Monitor	All	High
ELM archive process state change alert	306-50045	ELM compressing engine stopped or started.	Software Monitor	ADM/REC/DBM	Medium
ELM EDS FTP	306-50074	ELM SFTP program stopped or started.	Software Monitor	ELM	Medium

Rule name	Signature ID	Description	Type	Device	Severity
ELM file process	306-50065	ELM reinsertion engine stopped or started. If a log fails for any reason, it tries the insert again. If the process of reinsertion fails, this rule triggers.	Software Monitor	ELM	Medium
ELM mount point state change alert	306-50053	ELM remote storage (CIFS, NFS, ISCSI, SAN) stopped or started.	Software Monitor	ELM	Medium
ELM query engine state change alert	306-50046	ELM Jobs process – ELM jobs, such as ELM queries and inserts, stopped or started.	Software Monitor	ELM	Medium
ELM redundant storage	306-50063	ELM Mirror stopped or started.	Software Monitor	ELM	Medium
ELM system database error	306-50044	ELM database stopped or started.	Software Monitor	ELM	High
Email collector state change alert	306-50040	Cisco MARS collector stopped or started.	Software Monitor	Receiver	Medium
EPO tags applied	306-28	McAfee ePO tags applied.	Software Monitor	ESM	Low
Error communicating with ELM	306-50047	Communication with ELM failed.	Software Monitor	ADM/REC/DBM	High
Error in SSH communication	306-50077	Device issues such as version difference, change in key.	Software Monitor	All	High
ESM reboot	306-32	ESM rebooted.	Software Monitor	ESM	Medium
ESM shutdown	306-33	ESM shut down.	Software Monitor	ESM	Medium
eStreamer Collector alert	306-50070	eStreamer Collector stopped or started.	Software Monitor	Receiver	Medium
eStreamer Collector state change alert	306-50041	eStreamer Collector stopped or started.	Software Monitor	Receiver	Medium
Execute remote command	306-62	Alarm remote command executed.	Software Monitor	ESM	Low
Failed logon due to maximum concurrent sessions reached	306-37	User failed to log on because the maximum concurrent sessions were reached.	Software Monitor	ESM	High
Failed to format SAN device	306-50057	SAN on ELM failed to format; user must retry.	Hardware Monitor	ESM	High
Failed user logon	306-31	User failed to log on.	Software Monitor	ESM	Medium
File collector state change alert	306-50049	Mountcollector program stopped or started.	Software Monitor	Receiver	Medium
File deleted	306-50	Any file that can be added or removed	Software Monitor	ESM	Low
Filter process state change alert	306-50050	Filter program on the device stopped or started (filter rules).	Software Monitor	Receiver	Medium
Firewall alert aggregator state change alert	306-50009	Firewall aggregator on the ADM stopped or started.	Software Monitor	ADM	Medium

Rule name	Signature ID	Description	Type	Device	Severity
Get VA data failure	306-52	ESM failed to obtain VA data.	Software Monitor	ESM	Medium
Get VA data success	306-51	ESM obtained VA data.	Software Monitor	ESM	Low
Health monitor internal alert	306-50027	Health monitor process stopped or started.	Software Monitor	All	Medium
HTTP collector state change alert	306-50039	HTTP collector stopped or started.	Software Monitor	Receiver	Medium
Indexing configuration change	306-8	ESM indexing settings changed.	Software Monitor	ESM	Medium
Invalid SSH key	306-50075	Device issues communicating with ELM, such as version differences, change in key.	Software Monitor	All	High
IPFIX collector state change alert	306-50055	IPFIX (flow) collector stopped or started.	Software Monitor	Receiver	Medium
Key and certificate administrator user login	306-39	UCAPL event, Crypto administrator login.	Software Monitor	ESM	Low
Log partitions free disk space alert	306-50004	Log partition (/var) is low on free space.	Software Monitor	All	Medium
McAfee EDB database server state change alert	306-50010	Database stopped or started.	Software Monitor	All	Medium
McAfee ePO collector alert	306-50069	McAfee ePO collector stopped or started.	Software Monitor	Receiver	Medium
McAfee Event Format state change alert	306-50031	McAfee Event Format collector stopped or started.	Software Monitor	Receiver	Medium
McAfee SIEM device communication failure	306-26	ESM cannot communicate with another device.	Software Monitor	ESM	High
Microsoft Forefront Threat Management Gateway alert	306-50068	Forefront Threat Management Gateway collector stopped or started.	Software Monitor	Receiver	Medium
MS-SQL retriever state change alert	306-50035	Microsoft SQL collector stopped or started (any data source for Microsoft SQL).	Software Monitor	Receiver	Medium
Multi-event log alert	306-50062	jEMAIL collector stopped or started.	Software Monitor	Receiver	Medium
MVM scan initiated	306-27	MVM scan started.	Software Monitor	ESM	Low
NetFlow collector state change alert	306-50024	NetFlow (flow) collector stopped or started.	Software Monitor	Receiver	Medium
New user account	306-13	New user added to the system.	Software Monitor	ESM	Low
NFS/CIFS collector state change alert	306-50048	Remote mount for NFS or CIFS stopped or started.	Software Monitor	Receiver	Medium
NitroFlow collector state change alert	306-50026	NitroFlow (flows on device) stopped or started.	Software Monitor	Receiver	Medium
No SSH key found	306-50076	Device issues communicating with the ELM, such as version differences, change in key.	Software Monitor	All	High

Rule name	Signature ID	Description	Type	Device	Severity
NSM add/edit Blacklist	306-29	NSM Blacklist entry added or edited.	Software Monitor	ESM	Low
NSM delete Blacklist	306-30	NSM Blacklist entry deleted.	Software Monitor	ESM	Low
OPSEC retriever state change alert	306-50034	OPSEC (Check Point) collector stopped or started.	Software Monitor	Receiver	Medium
Oracle IDM collector alert	306-50072	Oracle IDM collector stopped or started.	Software Monitor	Receiver	Medium
Oversubscription alert	306-50012	ADM entered or exited oversubscription mode.	Software Monitor	ADM	Medium
Plug-in Collector/Parser alert	306-50073	Plug-in collector/parser stopped or started.	Software Monitor	Receiver	Medium
Policy add	306-15	Policy added to the system.	Software Monitor	ESM	Low
Policy delete	306-17	Policy deleted from the system.	Software Monitor	ESM	Low
Policy change	306-16	Policy changed in the system.	Software Monitor	ESM	Low
Previous configuration mismatch	146-6	Network discovery device configuration changed.	Software Monitor	ESM	Low
Receiver HA	306-50058	Any HA process stopped or started (Corosync, HA Control script).	Software Monitor	Receiver	Medium
Receiver HA Opsec configuration	306-50059	Not in use.	Software Monitor	Receiver	Low
Redundant ESM out of sync	306-76	Redundant ESM out of sync.	Software Monitor	ESM	High
Remote NFS mount point state change alert	306-50020	NFS ELM mount stopped or started.	Software Monitor	ELM	Medium
Remote share/mount point free disk space alert	306-50021	Free space on remote mount point is low.	Software Monitor	ESM	Medium
Remote SMB/CIFS share state change alert	306-50019	Remote SMB/CIFS mount point stopped or started.	Software Monitor	Receiver	Medium
Risk Correlation state change alert	306-50061	Risk Correlation engine stopped or started.	Software Monitor	ACE	Medium
Root partitions free disk space alert	307-50002	Free space on the root partitions is low.	Software Monitor	All	Medium
Rule add	306-20	Rule added to the system, such as ASP, filter, or correlation.	Software Monitor	ESM	Low
Rule delete	306-22	Rule deleted from the system.	Software Monitor	ESM	Low
Rule change	306-21	Rule changed in the system.	Software Monitor	ESM	Low
Rule update failure	306-9	ESM rule update failed.	Software Monitor	ESM	Medium
SDEE retriever state change alert	306-50033	SDEE collector stopped or started.	Software Monitor	Receiver	Medium

Rule name	Signature ID	Description	Type	Device	Severity
sFlow collector state change alert	306-50025	sFlow (flow) collector stopped or started.	Software Monitor	Receiver	Medium
SNMP collector state change alert	306-50023	SNMP collector stopped or started.	Software Monitor	Receiver	Medium
SQL collector state change alert	306-50038	SQL collector (old NFX) stopped or started.	Software Monitor	Receiver	Medium
Symantec AV collector state change alert	306-50056	Symantec AV collector stopped or started.	Software Monitor	Receiver	Medium
Syslog Collector state change alert	306-50037	Syslog collector stopped or started.	Software Monitor	Receiver	Medium
System admin user logon	306-40	System administrator logged on to the system.	Software Monitor	ESM	Low
System integrity check failure	306-50085	Non-ISO foreign program or process running on the system is flagged.	Software Monitor	All	High
System logger state change alert	306-50014	System logging process stopped or started.	Software Monitor	All	Medium
Task (query) closed	306-54	Task manager task closed.	Software Monitor	ESM	Low
Temporary partitions free disk space alert	306-50003	Temporary (/tmp) partition low on disk space.	Software Monitor	All	Medium
Text log parser state change alert	306-50052	Text parser process stopped or started.	Software Monitor	Receiver	Medium
User account change	306-14	User account changed.	Software Monitor	ESM	Low
User device failed logon	306-50079	SSH user failed to log on.	Software Monitor	ESM	Low
User device logon	306-50017	Not used in system.	Software Monitor	ESM	Low
User device logout	306-50078	SSH user logged out.	Software Monitor	ESM	Low
User logon	306-11	User logged on to the system.	Software Monitor	ESM	Low
User logout	306-12	User logged out of the system.	Software Monitor	ESM	Low
VA Data Engine status alert	306-50043	VA (vaded.pl) engine stopped or started.	Software Monitor	Receiver	Medium
Variable add	306-23	Policy variable added.	Software Monitor	ESM	Low
Variable delete	306-25	Policy variable deleted.	Software Monitor	ESM	Low
Variable change	306-24	Policy variable changed.	Software Monitor	ESM	Low
Web Server cert has expired	306-50084	ESM web server certificate expired.	Software Monitor	ESM	High
Web Server cert will expire soon	306-50083	ESM web server certificate expires soon.	Software Monitor	ESM	Medium

Rule name	Signature ID	Description	Type	Device	Severity
Websense collector alert	306-50067	Websense collector stopped or started.	Software Monitor	Receiver	Medium
WMI Event Log collector state change alert	306-50030	WMI collector stopped or started.	Software Monitor	Receiver	Medium

See also

[Add health monitor event alarms on page 256](#)

Add a Field Match alarm



A **Field Match** alarm matches on multiple fields of an event and triggers when the device receives and parses the event.

Before you begin

- Verify that you have administrator rights or belong to an access group with alarm management privileges.
- Review how to use logic elements.

For details about product features, usage, and best practices, click **?** or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
 - 2 Click **Alarms**.
 - 3 Click **Add**, type the alarm name and select the assignee, then click the **Condition** tab.
 - 4 In the **Type** field, select **Field Match**, then set up the conditions for the alarm.
 - a Drag and drop the **AND** or **OR** to set up the logic for the alarm's condition.
 - b Drag and drop the **Match Component** icon onto the logic element, then complete the **Add Filter Field** page.
 - c In the **Maximum Condition Trigger Frequency** field, select the amount of time to allow between each condition to prevent a flood of notifications. Each trigger only contains the first source event that matches the trigger condition, not the events that occurred within the trigger frequency period. New events that match the trigger condition do not cause the alarm to trigger again until after the maximum trigger frequency period.
-  If you set the interval to zero, every event that matches a condition triggers an alarm. For high frequency alarms, a zero interval can produce many alarms.
- 5 Click **Next** and select the devices to be monitored for this alarm. This alarm type supports Receivers, local Receiver-Enterprise Log Managers (ELMs), Receiver/ELM combos, ACEs, and Application Data Monitors (ADMs).
 - 6 Click the **Actions** and **Escalation** tabs to define the settings.
 - 7 Click **Finish**.

The alarm writes out to the device.



If the alarm fails to write out to the device, an out-of-sync flag appears next to the device in the system navigation tree. Click the flag, then click **Sync Alarms**.

Table 7-4 Option definitions

Option	Definition
Radio buttons	Change the logical element type. This is helpful if you have a rule or component with several layers of logic elements and then realize that one of the elements at the beginning of the logic diagram should be a different type.
conditions	Select the number of conditions that must be met for a SET with more than one condition.
Sequence	Select if you want the conditions of the AND or SET logical element to occur in the sequence you place them in the Correlation Logic field for the rule to be triggered.
Threshold	Set the number of times the conditions need to occur for the rule to trigger.
Time Window	Set the time limit that the threshold needs to occur in for the rule to trigger.


See also

[Customize summary for triggered alarms and cases on page 265](#)

[Logic elements on page 264](#)

Logic elements

When you add an Application Data Monitor (ADM), database, and correlation rule or component, use **Expression Logic** or **Correlation Logic** to build the rule's framework.

Element	Description
 AND	Functions the same as a logical operator in a computer language. Everything that is grouped under this logical element must be true for the condition to be true. Use this option if you want all conditions under this logical element to be met before a rule is triggered.
OR	Functions the same as a logical operator in a computer language. Only one condition grouped under this element has to be true for this condition to be true. Use this element if you want only one condition to be met before the rule is triggered.
SET	For correlation rules or components, SET allows you to define conditions and select how many conditions must be true to trigger the rule. For example, if two conditions out of three in the set must be met before the rule is triggered, the set reads "2 of 3."

Each of these elements has a menu with at least two of these options:

- **Edit** — You can edit the default settings (see *Edit logic elements default settings*).
- **Remove logical element** — You can delete the selected logical element. If it has any children, they aren't deleted and move up in the hierarchy.



This doesn't apply to the root element (the first one in the hierarchy). If you remove the root element, all children are also removed.

- **Remove logical element and all of its children** — You can delete the selected element and all its children from the hierarchy.

When you set up the rule's logic, you must add components to define the conditions for the rule. For correlation rules, you can also add parameters to control the behavior of the rule or component when it executes.

See also

[Add a Field Match alarm on page 263](#)

[Edit logical elements on page 367](#)

Customize summary for triggered alarms and cases




Select the data to include in the alarm summary and the case summary of **Field Match** and **Internal Event Match** alarms.

Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**, then click **Add**.
- 3 On the **Condition** tab, select the **Field Match** or **Internal Event Match** type.
- 4 Click the **Actions** tab, click **Create a case for**, click the variables icon , then select the fields to include in the case summary.
- 5 Click **Customize triggered alarm summary**, click the variables icon , then select the fields to include in the summary for the triggered alarm.
- 6 Type the information requested to create alarms, then click **Finish**.

See also

[Add a Field Match alarm on page 263](#)

Add an alarm to rules



To be notified when events are generated by specific rules, you can add an alarm to those rules.

Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, click the **Policy Editor** icon  on the actions toolbar.
- 2 Select the type of rule in the **Rule Types** pane.
- 3 Select one or more rules in the rules display area.
- 4 Click the **Alarms** icon .
- 5 Create the alarm.

Create SNMP traps as alarm actions


Send SNMP traps as an alarm action.

Before you begin

- Verify that you have administrator rights or belong to an access group with alarm management privileges.
- Prepare the SNMP trap Receiver (only required if you don't have an SNMP trap Receiver).

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 Create an SNMP profile to tell the ESM where to send the SNMP traps.
 - a On the system navigation tree, select the system, then click the **Properties** icon .
 - b Click **Profile Management**, then select **SNMP Trap** in the **Profile Type** field.
 - c Fill in the remaining fields, then click **Apply**.
- 2 Configure SNMP on the ESM.
 - a On **System Properties**, click **SNMP Configuration**, then click the **SNMP Traps** tab.
 - b Select the port, select the types of traps to send, then select the profile you added in Step 1.
 - c Click **Apply**.
- 3 Define an alarm with **SNMP Trap** as an action.
 - a On **System Properties**, click **Alarms**, then click **Add**.
 - b Fill in the information requested on the **Summary**, **Condition**, and **Devices** tabs, selecting **Internal Event Match** as the condition type, then click the **Actions** tab.
 - c Select **Send Message**, then click **Configure** to select or create a template for SNMP messages.
 - d Select **Basic SNMP Templates** in the **SNMP** field, or click **Templates**, and select an existing template or click **Add** to define a new template.
 - e Return to the **Alarm Settings** page, then proceed with alarm setup.

Add a power failure notification alarm


Add an alarm to notify you when either of the ESM power supplies fail.

Before you begin

- Verify that you have administrator rights or belong to an access group with alarm management privileges.
- [Set up SNMP trap for power failure notification](#) on page 181

For details about product features, usage, and best practices, click ? or **Help**.

Task

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Alarms**.

- 3 Click **Add**, enter the requested data on the **Summary** tab, then click the **Condition** tab.
- 4 In the **Type** field, select **Internal Event Match**.
- 5 In the **Field** field, select **Signature ID**, then type 306-50086 in the **Value(s)** field.
- 6 Enter the remaining information as needed for each tab, then click **Finish**.

An alarm triggers when a power supply fails.

Manage out-of-sync data sources

Set up an alarm to alert you when out-of-sync data sources generate events so that you can view a list of data sources, edit their settings, and export the list.


Before you begin

Verify that you have administrator rights or belong to an access group with alarm management privileges.

This diagnostic tool identifies when a data source is collecting past or future events, which can cause a red flag to appear on the Receiver.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Set up an alarm to notify you when an event comes into the Receiver, generated by a data source that is out of sync with the ESM.
 - a Click **Alarms | Add**, type the information requested on the **Summary** tab, then click the **Condition** tab.
 - b Select **Event Delta** in the **Type** field, select how often the ESM should check for out-of-sync data sources, and select the time difference that must exist for the alarm to trigger.
 - c Complete the information in the remaining tabs.
- 3 View, edit, or export the data sources that are out of sync.
 - a On the system navigation tree, click the Receiver, then click the **Properties** icon.
 - b Click **Receiver Management**, then click **Time Delta**.

See also

[Out-of-sync data sources on page 267](#)

Out-of-sync data sources

As a result of several possible settings, the time on a data source can get out of sync with the ESM. When an out-of-sync data source generates an event, a red flag appears next to the Receiver on the system navigation tree.

You can set up an alarm to notify you when this occurs. You can then manage the data sources that are out of sync by accessing the **Time Delta** page (see *Manage out-of-sync data sources*).



Out-of-sync events can be old events or future events.

Your data sources can be out of sync with the ESM for several reasons.

- 1 The ESM has the incorrect time zone setting (see *Select user settings*).
- 2 You set the time to the wrong zone when adding the data source (see *Add a data source*).
- 3 The system has been on for a long time and the timing slips out of sync.
- 4 You set up the system that way on purpose.
- 5 The system isn't connected to the Internet.
- 6 The event is out of sync when it comes into the Receiver.

Table 7-5 Option definitions

Option	Definition
Table	Lists the data sources, IP addresses or host names, type of data source, and the time delta for the events.
Edit	Opens the Edit Data Source page for the selected data source. You can change the time zone setting so that the data source generates events with the correct time.
Export	Exports the list in the table.
Refresh	Updates the information in the table to reflect recent changes.
Interval	Determines how far back in the database events are analyzed.

See also

[Manage out-of-sync data sources on page 267](#)

8

Working with events

ESM enables you to identify, collect, process, correlate, and store billions of events and flows, keeping all information available for queries, forensics, rules validation, and compliance.

Contents

- *Events, flows, and logs*
- *Managing reports*
- *Description of contains and regex filters*
- *Working with ESM views*
- *Custom type filters*
- *McAfee® Active Response searches*

Events, flows, and logs

Events, flows, and logs record different types of activities that occur on a device.

An *event* is an activity recorded by a device as a result of a rule on your system. A *flow* is the record of a connection made between IPs, at least one of which is on your HOME_NET. A *log* is a record of an event that occurred to a device on your system. Events and flows have source and destination IP addresses, ports, Media Access Control (MAC) addresses, a protocol, and a first and last time. But, there are several differences between events and flows:

- Because flows are not an indication of anomalous or malicious traffic, they are more common than events.
- A flow is not associated with a rule signature (SigID) like an event is.
- Flows are not associated with event actions such as alert, drop, and reject.
- Certain data is unique to flows, including source and destination bytes, and source and destination packets. *Source bytes and packets* are the number of bytes and packets transmitted by the source of the flow. The *destination bytes and packets* are the number of bytes and packets transmitted by the destination of the flow.
- Flows have direction: An *inbound flow* is defined as a flow that originates from outside of the HOME_NET. An *outbound flow* originates from inside the HOME_NET.

Events and flows generated by the system can be seen on views, which you can select on the views list. Logs are listed on the **System Log** or **Device Log** accessed from the **Properties** page for the system or each device.

See also

Set up events, flows, and logs downloads on page 270

Limit time for data collection on page 271

Define inactivity threshold settings on page 271

Get events and flows on page 272

Check for events, flows, and logs on page 273

Define geolocation and ASN settings on page 274

Set up events, flows, and logs downloads

Check for events, flows, and logs manually or set the device to check for them automatically.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).



- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Events, Flows & Logs**, **Events & Logs**, or **Logs**.
- 3 Set up the downloads, then click **Apply**.

Table 8-1 Option definitions

Option	Definition
Auto Update Rules	If the ESM automatically downloads rules from the rules server, select this option if you want the downloaded rules to be rolled out to this device.
Auto Download...	Select if you want the ESM to check for events, flows, or logs automatically.
Get...	Click if you want the ESM to check for events, flows, or logs now. To view the status of these jobs, see <i>Get Events and Flows</i> .
Define daily data pull time range	<p>Select to schedule a daily time range for the ESM to pull data from each device and to send data to the ELM from each device (see <i>Limit collection time for data</i>).</p> <div>  Be careful when configuring this feature because scheduling event, flow, and log collection might result in data loss. </div>
Generate Vulnerability Events	Select to have events that match vulnerability assessment source data added to the system (see <i>Work with vulnerability assessment</i>), become a vulnerability event, and generate an alert on the Local ESM. The policy properties on the Policy Editor are the same for each of these events and can't be changed (for example, severity is always 100).
Last Event or Flow Download Process	See the last time events or flows were retrieved from the device, whether the process was successful, and the number of events or flows retrieved.
Last Downloaded Event, String, or Flow Record	See the date and time of the last event, string, or flow record retrieved. Changing this value allows you to set the date and time from which you want to retrieve events, strings, or flows. For example, if you enter November 13, 2016 at 10:30:00 AM in the Last Downloaded Event Record field, click Apply , then click Get Events , the ESM retrieves events on this device from that time to date.
Database Settings	Click to manage database index settings on the ESM.
Inactivity Settings	View and change the inactivity threshold settings for each device managed by the ESM (see <i>Define inactivity threshold settings</i>).
Geolocation	Set up the ESM to log geolocation and ASN data for each device (see <i>Define geolocation and ASN settings</i>).

See also

[Events, flows, and logs](#) on page 269

[Limit time for data collection](#) on page 271

[Define inactivity threshold settings](#) on page 271

[Get events and flows](#) on page 272

[Check for events, flows, and logs](#) on page 273

[Define geolocation and ASN settings](#) on page 274

Limit time for data collection

You can schedule a daily time range to limit when the ESM pulls data from each device and when data is sent to the ELM from each device.


You can use this feature to avoid using the network at peak times, leaving the bandwidth available for other applications. This does delay data delivery to the ESM and ELM, so determine if this delay is acceptable in your environment.

Task



Be careful when configuring this feature because scheduling event, flow, and log collection might result in data loss.

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the device, then click the **Properties** icon .
- 2 Select one of the following:
 - **Events, Flows & Logs**
 - **Events & Logs**
 - **Logs**
- 3 Select **Define daily data pull time range**, then set the start time and end time for the time range.

The ESM collects data from the device and the device sends data to the ELM for logging during the time range you defined. When you set this up on an ELM, it defines when the ESM collects data from the ELM and when the ESM sends data to the ELM for logging.

See also

[Events, flows, and logs on page 269](#)

[Set up events, flows, and logs downloads on page 270](#)

[Define inactivity threshold settings on page 271](#)

[Get events and flows on page 272](#)

[Check for events, flows, and logs on page 273](#)

[Define geolocation and ASN settings on page 274](#)

Define inactivity threshold settings

When you set an inactivity threshold for a device, you are notified when no events or flows are generated in the specified period of time. If the threshold is reached, a yellow health status flag appears next to the device node on the system navigation tree.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, make sure that **System Information** is selected, then click **Events, Flows, & Logs**.
- 2 Click **Inactivity Settings**.

- 3 Highlight the device, then click **Edit**.
- 4 Make changes to the settings, then click **OK**.

Table 8-2 Option definitions

Option	Definition
Device column	Lists all the device on your system.
Threshold column	Shows the threshold for each device.
Inherit column	Shows if a child device inherits its parent's threshold setting. Select or deselect to change the setting.
Edit	Opens the Edit Inactivity Threshold page so you can change the threshold setting.

See also

Events, flows, and logs on page 269

Set up events, flows, and logs downloads on page 270

Limit time for data collection on page 271

Get events and flows on page 272

Check for events, flows, and logs on page 273


Define geolocation and ASN settings on page 274

Get events and flows

Retrieve events and flows for the devices you select on the system navigation tree.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the system, a group, or a device, then click the **Get Events and Flows** icon  on the actions toolbar.

- 2 In the top table, select the events and flows to be retrieved, then click **Start**.

The status of the retrieval is reflected in the **Status** column. The bottom table shows further details for the devices you highlight in the top table.



- 3 When the download is complete, select a view to display these events and flows in, then click the **Refresh Current View** icon  on the views toolbar.

Table 8-3 Option definitions

Option	Definition
	Minimize the Get Events and Flows page as it continues to retrieve the events or flows.
TOP TABLE	
Device Name column	View the devices you can retrieve events or flows for based on what you selected in the system navigation tree. You can select one or more of these devices to view details in the bottom table.
Events column	Select the devices you want to retrieve events for.
Flows column	Select the devices you want to retrieve flows for.
Status column	View the status of the retrieval after you start it. It lists the number of insert jobs and get jobs running against a device, and the last get job that ran while the window was open. It refreshes every two seconds.
Start	Click to begin the retrieval. At least one checkbox must be selected for this option to be active.
Cancel	Cancel the process once it has started. The process stops after the current operation is completed.
BOTTOM TABLE	
Device Name column	View the names of the devices that are selected in the top table.
Operation column	View the current operation being performed on the device.
Start Time column	View the time that the job was created, which is not necessarily the time that the job began processing on the ESM.
Status column	View the status of the job.
Refresh	Update the table. It is refreshed automatically every five seconds.

See also

Events, flows, and logs on page 269

Set up events, flows, and logs downloads on page 270

Limit time for data collection on page 271

Define inactivity threshold settings on page 271

Check for events, flows, and logs on page 273

Define geolocation and ASN settings on page 274

Check for events, flows, and logs

You can set the ESM to check for events, flows, and logs automatically or you can check for them manually. The rate at which you check for them depends on your system's level of activity and how often you want to receive

status updates. You can also specify which devices should check for each type of information and set the inactivity threshold settings for the devices managed by the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Events, Flows, & Logs**.
- 2 Make the selections and changes for event, flow, and log retrieval.
- 3 Click **OK**.

Table 8-4 Option definitions

Option	Definition
Auto check every	Select if you want the system to check for events, flows, and logs automatically. Set the frequency for how often you want it done.
Check now	Check for events, flows, and logs now.
Show Devices	Select the automatic download settings for events, flows, and logs for each device.
Inactivity Settings	If you want to be notified when a device hasn't generated events or flows for a period of time, select this option, highlight the device, then click Edit .

Table 8-5 Option definitions

Option	Definition
Device Name column	Lists all the devices on the system
Events column	Select the devices that you want to automatically download events.
Flow column	Select the devices that you want to automatically download flows.
Logs column	Select the devices that you want to automatically download logs.

See also

Events, flows, and logs on page 269

Set up events, flows, and logs downloads on page 270

Limit time for data collection on page 271

Define inactivity threshold settings on page 271

Get events and flows on page 272

Define geolocation and ASN settings on page 274


Define geolocation and ASN settings

Geolocation provides the geographic location of computers connected to the Internet. *Autonomous System Number (ASN)* is a number that is assigned to an autonomous system and uniquely identifies each network on the Internet.

Both of these types of data can help you identify the physical location of a threat. Source and destination geolocation data can be collected for events.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Events, Flows & Logs** or **Events & Logs**, then click **Geolocation**.
- 3 Make the selections to generate the information needed, then click **OK**.

You can filter event data using this information.

Table 8-6 Option definitions

Option	Definition
Collect geolocation data	To collect geolocation data for events or flows, select this option.
Source data, Destination data	If you clicked Collect geolocation data , select if you want to collect either of these or both.
Collect ASN data	To collect ASN data for events or flows, select this option.
Source data, Destination data	If you clicked Collect ASN data , select if you want to collect either of these or both.
Off	Select if you want to stop collection of geolocation or ASN data for events or flows.
Refresh	Click to return to the current device settings.

See also

[Events, flows, and logs on page 269](#)

[Set up events, flows, and logs downloads on page 270](#)

[Limit time for data collection on page 271](#)

[Define inactivity threshold settings on page 271](#)

[Get events and flows on page 272](#)

[Check for events, flows, and logs on page 273](#)

Aggregating events or flows

An event or flow can potentially be generated thousands of times. Instead of sifting through thousands of identical events, you can view them as a single event or flow with a count that indicates the number of times it occurred.

Using aggregation uses disk space on both the device and ESM more efficiently because it eliminates the need to store each packet. This feature applies only to rules that have aggregation enabled in the **Policy Editor**.

Source IP address and destination IP address

The source IP address and destination IP address "not-set" values or aggregated values appear as ":::" instead of as "0.0.0.0" in all result sets. For example:

- ::ffff:10.0.12.7 is inserted as 0:0:0:0:0:FFFF:A00:C07 (A00:C07 is 10.0.12.7).
- ::0000:10.0.12.7 would be 10.0.12.7.

Aggregated events and flows


Aggregated events and flows use the first, last, and total fields to indicate the duration and amount of aggregation.

For example, if the same event occurred 30 times in the first 10 minutes after noon, the **First time** field contains the time 12:00 (the time of the first instance of the event), the **Last time** field contains the time 12:10 (the time of the last instance of the event), and the **Total** field contains the value 30.

You can change the default event or flow aggregation settings for the device as a whole. For events, you can add exceptions to the device's settings for individual rules.

Aggregation retrieves records based on the events, flows, and logs retrieval setting. If it is set for automatic retrieval, the device compresses a record only until the first time the ESM pulls it. If it is set for manual retrieval, a record compresses up to 24 hours or until a new record is pulled manually, whichever comes first. If the compression time reaches the 24-hour limit, a new record is pulled and compression begins on that new record.

Table 8-7 Option definitions

Option	Definition
Auto Update Rules	If the ESM automatically downloads rules from the rules server, select this option if you want the downloaded rules to be rolled out to this device.
Auto Download...	Select if you want the ESM to check for events, flows, or logs automatically.
Get...	Click if you want the ESM to check for events, flows, or logs now. To view the status of these jobs, see <i>Get Events and Flows</i> .
Define daily data pull time range	Select to schedule a daily time range for the ESM to pull data from each device and to send data to the ELM from each device (see <i>Limit collection time for data</i>). <div>  Be careful when configuring this feature because scheduling event, flow, and log collection might result in data loss. </div>
Generate Vulnerability Events	Select to have events that match vulnerability assessment source data added to the system (see <i>Work with vulnerability assessment</i>), become a vulnerability event, and generate an alert on the Local ESM. The policy properties on the Policy Editor are the same for each of these events and can't be changed (for example, severity is always 100).
Last Event or Flow Download Process	See the last time events or flows were retrieved from the device, whether the process was successful, and the number of events or flows retrieved.
Last Downloaded Event, String, or Flow Record	See the date and time of the last event, string, or flow record retrieved. Changing this value allows you to set the date and time from which you want to retrieve events, strings, or flows. For example, if you enter November 13, 2016 at 10:30:00 AM in the Last Downloaded Event Record field, click Apply , then click Get Events , the ESM retrieves events on this device from that time to date.
Database Settings	Click to manage database index settings on the ESM.
Inactivity Settings	View and change the inactivity threshold settings for each device managed by the ESM (see <i>Define inactivity threshold settings</i>).
Geolocation	Set up the ESM to log geolocation and ASN data for each device (see <i>Define geolocation and ASN settings</i>).

See also

[Change event or flow aggregation settings on page 276](#)

[Add exceptions to event aggregation settings on page 277](#)

[Manage event aggregation exceptions on page 278](#)

Change event or flow aggregation settings

Event aggregation and flow aggregation are enabled by default, and are set on **Medium High**. You can change the settings as needed. The performance of each setting is described on the **Aggregation** page.

Before you begin

You must have **Policy Administrator** and **Device Management** or **Policy Administrator** and **Custom Rules** rights to change these settings.



Event aggregation is available only for ADM and Receiver devices, and flow aggregation for Receiver devices.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Event Aggregation** or **Flow Aggregation**.
- 3 Define the settings, then click **OK**.

Table 8-8 Option definitions

Option	Definition
Refresh	Click to read the current aggregation settings on the device. It then uses the aggregation rate.
Sliding scale	Click the indicator arrow and drag it to the setting. The description for levels 2 and 3 change to reflect the settings you select.
Custom setting on the sliding scale	Set Level 2 and Level 3 values.
Apply	Update the device with all settings on this screen.
View (events only)	Open the Event Aggregation Exceptions page (see <i>Add exception to event aggregation settings</i>).
Ports (flows only)	Configure the flow port aggregation values that need to be maintained (see <i>Configure flow port aggregation values</i>).

See also

[Aggregating events or flows on page 275](#)

[Add exceptions to event aggregation settings on page 277](#)


[Manage event aggregation exceptions on page 278](#)

Add exceptions to event aggregation settings

Aggregation settings apply to all events generated by a device. You can create exceptions for individual rules if the general settings don't apply to the events generated by that rule.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the views pane, select an event generated by the rule you want to add an exception for.
- 2 Click the **Menu** icon , then select **Modify Aggregation Settings**.
- 3 Select the field types you want to aggregate from the **Field 2** and **Field 3** drop-down lists.



The fields you select in **Field 2** and **Field 3** must be different types or an error results. When you select these field types, the description for each aggregation level changes to reflect the selections you made. The time limits for each level depend on the event aggregation setting you defined for the device.

- 4 Click **OK** to save your settings, then click **Yes** to proceed.
- 5 Deselect devices if you do not want to roll out the changes to them.
- 6 Click **OK** to roll out the changes to the devices that are selected.

The **Status** column shows the status of the update as the changes are rolled out.

Table 8-9 Option definitions

Option	Definition
Edit	Click to make changes to the selected exception.
Remove	Delete the selected exception.
Rollout	Roll out the changes to the device.

Table 8-10 Option definitions

Option	Definition
Device column	View the devices on the system.
second column	Select the devices you want to roll the changes out to.
Status column	View the status of the rollout for each device.

See also

[Aggregating events or flows on page 275](#)

[Change event or flow aggregation settings on page 276](#)


[Manage event aggregation exceptions on page 278](#)

Manage event aggregation exceptions

You can view a list of the event aggregation exceptions that were added to the system. You can also edit or remove an exception.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select a device, then click the **Properties** icon .
- 2 Click **Event Aggregation**, then click **View** at the bottom of the screen.
- 3 Make the needed changes, then click **Close**.

See also

[Aggregating events or flows on page 275](#)

[Change event or flow aggregation settings on page 276](#)

[Add exceptions to event aggregation settings on page 277](#)

Setting up event forwarding

Event forwarding allows you to send events from the ESM to another device or facility by Syslog or SNMP (if enabled). You must define the destination, and can select if you want to include the packet and obfuscate the IP data. You can add filters so the event data is filtered before it is forwarded.

This isn't a substitute for log management, because it's not a full set of digitally signed logs from each device in your environment.

See also

[Event forwarding agents on page 281](#)

[Sending and forwarding events with Standard Event Format on page 284](#)

[Configure event forwarding on page 279](#)

[Add event forwarding destinations on page 279](#)

[Enable or disable event forwarding on page 282](#)

[Modify settings for all event forwarding destinations on page 282](#)

[Add event forwarding filters on page 282](#)

[Edit event forwarding filter settings on page 283](#)

Configure event forwarding

You can set up an event forwarding destination to forward event data to a syslog or SNMP server.



The number of event forwarding destinations in use, in combination with the rate and number of events that are being retrieved by your ESM, can affect overall ESM performance.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
- 2 On the **Event Forwarding Destinations** page, select **Add**, **Edit**, or **Remove**.
- 3 If you selected to add or edit a destination, define the settings.
- 4 Click **Apply** or **OK**.

Table 8-11 Option definitions

Option	Definition
Event Forwarding Destinations	View the destinations that have been added to the system.
Add	Add a destination to the system.
Edit	Change the settings of the destination you select.
Remove	Delete a destination from the system.
Settings	Specify settings that apply to all event forwarding destinations.

See also

[Setting up event forwarding on page 278](#)

[Event forwarding agents on page 281](#)

[Sending and forwarding events with Standard Event Format on page 284](#)

[Add event forwarding destinations on page 279](#)

[Enable or disable event forwarding on page 282](#)

[Modify settings for all event forwarding destinations on page 282](#)

[Add event forwarding filters on page 282](#)

[Edit event forwarding filter settings on page 283](#)

Add event forwarding destinations

Add an event forwarding destination to the ESM to forward event data to a syslog or SNMP server.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
- 2 Click **Add**, then fill in the requested information.
- 3 Click **OK**.

Table 8-12 Option definitions

Option	Definition
Name	Enter a name for this destination.
Enabled	Select to enable event forwarding to this destination.
Use System Profile	Select to use an existing profile, then select a profile from the drop-down list or click Use System Profile to add a new profile.
Format	Select the format on the drop-down list. See <i>Event Forwarding Agents</i> for a detailed list of the agents and the information contained within the packets.
Destination IP Address	Type the destination IP address of the syslog.
Destination Port	Select the destination port the syslog is listening on.
Protocol	<p>Choose between the UDP or TCP transport protocols. UDP is the protocol standard syslog is based on. Packets sent via syslog over TCP are formatted exactly like their UDP counterparts including facility, severity, and message, the only exception being a new line character (ASCII character code 10) appended to the end of the message.</p> <p>Unlike UDP, which is a connectionless protocol, a TCP connection must be established between the ESM and the server listening for the forwarded events. If a connection can't be established or the connection is dropped, the ESM keeps track of the last event successfully forwarded, and tries to establish the connection again in a few minutes. Once the connection is reestablished, the ESM picks up forwarding event where it left off.</p> <p>If you select UDP, you will not be able to select SSH or TLS in the Mode field.</p>
Facility	Select the facility of the syslog packets.
Severity	Select the severity of the syslog packets.
Time Format	Select the time format for the header of syslog event forwarding. If you select Legacy , the format will be the same as it was in versions prior to 9.3.0, which was GMT. If you select Standard , you can select a time zone.
Time Zone	If you selected Standard , select the time zone to be used when sending event forwarding logs.
Obfuscate data	Select to mask selected data included in the data forwarded to this destination. To select the data, click Configure .
Send Packet	If you have your policy set to copy a packet, select this option to forward the packet information. This information is included, if the packet is available, at the end of the syslog message in Base 64 encoding.
Event Filters	Click to apply filters to the event data that is forwarded to a syslog.
Mode	Select the security mode for the message. If you select SSH, fill in the remaining information. If you choose to use syslog over TCP (protocol), select to make the TCP connection using SSH or TLS. As syslog is an unencrypted protocol, using SSH or TLS prevents your event forwarding messages from being examined by other parties. If you are in FIPS mode, you can forward log data using TLS.
Local Relay Port	Type the port to use on the ESM side of the SSH connection.

Table 8-12 Option definitions (continued)

Option	Definition
Remote SSH Port	Type the port that the SSH server is listening on the other side of the SSH connection.
SSH Username	Type the SSH user name used to establish the SSH connection.
SSH DSA Key	Type the public DSA authentication key used for SSH authentication. The contents of this field is added to the authorized_keys file or equivalent on the machine running the SSH server.

See also

[Setting up event forwarding on page 278](#)

[Event forwarding agents on page 281](#)

[Sending and forwarding events with Standard Event Format on page 284](#)

[Configure event forwarding on page 279](#)

[Enable or disable event forwarding on page 282](#)

[Modify settings for all event forwarding destinations on page 282](#)

[Add event forwarding filters on page 282](#)

[Edit event forwarding filter settings on page 283](#)

Event forwarding agents

These are the event forwarding agents and the information contained in the packets when they are forwarded. You select the agent in the **Format** field on the **Add Event Forwarding Destination** page.

Agent	Contents
Syslog (Audit Logs)	time (seconds since the epoch), status flag, user name, log category name (blank for 8.2.0, populated for 8.3.0+), device group name, device name, log message.
Syslog (Common Event Format)	Current date and time, ESM IP, CEF version 0, vendor = McAfee, product = ESM model from /etc/McAfee Nitro/ipsmodel, version = ESM version from /etc/buildstamp, sig id, sig message, severity (0 to 10), name/value pairs, deviceTranslatedAddress
Syslog (Standard Event Format)	<#>YYYY-MM-DDTHH:MM:SS.S [IP Address] McAfee_SIEM: <pre>{ "source": { "id": 144120685667549200, "name": "McAfee Email Gateway (ASP)", "subnet": "::ffff:10.75.126.2/128" }, "fields": { "packet": { "encoding": "BASE64" } }, "data": { "unique_id": 1, "alert_id": 1, "thirdpartytype": 49, "sig": { "id": 5000012, "name": "Random String Custom Type" }, "norm_sig": { "id": 1343225856, "name": "Misc Application Event" }, "action": "5", "src_ip": "65.254.48.200", "dst_ip": "0.0.0.0", "src_port": 38129, "dst_port": 0, "protocol": "n/a", "src_mac": "00:00:00:00:00:00", "dst_mac": "00:00:00:00:00:00", "src_asn_geo": 1423146310554370000, "firsttime": "2014-05-09T20:43:30Z", "lasttime": "2014-05-09T20:43:30Z", "writetime": "2014-05-09T20:44:01Z", "src_guid": "", "dst_guid": "", "total_severity": 25, "severity": 25, "eventcount": 1, "flow": "0", "vlan": "0", "sequence": 0, "trusted": 2, "session_id": 0, "compression_level": 10, "reviewed": 0, "a1_ran_string_CF1": "This is data for custom field 1", "packet": "PDE0PjA5MDUyMDE0IDlwOjE4OjQ0fDlxYDY1LjI1NC40OC4yMDAtMzgxmjl8MXwxMDJ8U3BhbSBnZXNzYWdlIHRS5cGU6IFRydXN0ZWRTb3VyY2UgU2lnbmF0dXJlIENvbmZpZGVuY2UgPSBISUdlLiBDb25uZWNOaW9uOiA2NS4yNTQNdGUmjAwLTMT5KElQLVBvcnQpfFRoaXMgaXMGZGF0YSBm b3JlY3VzdG9tIGZpZWxkIDF8W10A"</pre>

See also

[Setting up event forwarding on page 278](#)

[Sending and forwarding events with Standard Event Format on page 284](#)

[Configure event forwarding on page 279](#)

[Add event forwarding destinations on page 279](#)

[Enable or disable event forwarding on page 282](#)

[Modify settings for all event forwarding destinations on page 282](#)

[Add event forwarding filters on page 282](#)

[Edit event forwarding filter settings on page 283](#)

Enable or disable event forwarding

Enable or disable event forwarding on the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
- 2 Click **Settings**, then select or deselect **Event Forwarding Enabled**.
- 3 Click **OK**.

See also

Setting up event forwarding on page 278

Event forwarding agents on page 281

Sending and forwarding events with Standard Event Format on page 284

Configure event forwarding on page 279

Add event forwarding destinations on page 279

Modify settings for all event forwarding destinations on page 282

Add event forwarding filters on page 282

Edit event forwarding filter settings on page 283

Modify settings for all event forwarding destinations

Change some settings for all existing event forwarding destinations at one time.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
- 2 Click **Settings**, then set the options.
- 3 Click **OK**.

See also

Setting up event forwarding on page 278

Event forwarding agents on page 281

Sending and forwarding events with Standard Event Format on page 284

Configure event forwarding on page 279

Add event forwarding destinations on page 279

Enable or disable event forwarding on page 282

Add event forwarding filters on page 282

Edit event forwarding filter settings on page 283

Add event forwarding filters


Set up filters to limit the event data forwarded to a syslog or SNMP server on the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
- 2 Click **Add**, then click **Event Filters**.
- 3 Fill in the filter fields, then click **OK**.

Table 8-13 Option definitions

Option	Definition
Device	Click the filter icon  , select the device to filter by, then click OK .
Destination IP	Type an individual destination IP address (161.122.15.13) or a range of IP addresses (192.168.0.0/16) to filter by.
Destination Port	Type the filter port; one is allowed.
Protocol	Type the filter protocol; one is allowed.
Source IP	Type the individual source IP address or a range of IP addresses to filter by.
Device Type	Click the filter icon, select a maximum of 10 device types, then click OK .
Normalized ID	Select normalized IDs for filtering (see <i>What are Normalized IDs</i>).
Severity	To filter by an event severity, select Greater than or equal and a severity number between 0 and 100.

See also

Setting up event forwarding on page 278

Event forwarding agents on page 281

Sending and forwarding events with Standard Event Format on page 284

Configure event forwarding on page 279

Add event forwarding destinations on page 279

Enable or disable event forwarding on page 282

Modify settings for all event forwarding destinations on page 282

Edit event forwarding filter settings on page 283

Edit event forwarding filter settings

Change filter settings for event forwarding after they are saved.

Before you begin

When editing a device filter, you must have access to all the devices in the filter. To enable access to the devices, see *Set up user groups*.

Task

For details about product features, usage, and best practices, click ? or **Help**.



- 1 On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
- 2 Click **Edit**, then click **Event Filters**.
- 3 Make the changes, then click **OK**.

See also[Setting up event forwarding on page 278](#)[Event forwarding agents on page 281](#)[Sending and forwarding events with Standard Event Format on page 284](#)[Configure event forwarding on page 279](#)[Add event forwarding destinations on page 279](#)[Enable or disable event forwarding on page 282](#)[Modify settings for all event forwarding destinations on page 282](#)[Add event forwarding filters on page 282](#)**Sending and forwarding events with Standard Event Format**

Standard Event Format (SEF) is a Java Script Object Notation (JSON)-based event format to represent generic event data.

SEF format forwards events from the ESM to a Receiver on a different ESM, as well as from the ESM to a third party. You can also use it to send events from a third party to a Receiver by selecting SEF as the data format when creating the data source.

When setting up event forwarding with SEF from ESM to ESM, you need to perform four steps:

- 1 Export data sources, custom types, and custom rules from the ESM that is forwarding the events.
 - To export the data sources, follow the instructions in *Move data sources to another system*.
 - To export the custom types, open **System Properties**, click **Custom Types**, then click **Export**.
 - To export the custom rules, follow the instructions in *Export rules*.
- 2 On the ESM with the Receiver you are forwarding to, import the data sources, custom types, and custom rules that you just exported.
 - To import the data sources, follow the instructions in *Move data sources to another system*.
 - To import the custom types, open **System Properties**, click **Custom Types**, then click **Import**.
 - To import the custom rules, follow the instructions in *Import rules*.
- 3 On the ESM that is receiving the events from another ESM, add an ESM data source.
 - On the system navigation tree, click the Receiver device you want to add the data source to, then click the **Add Data Source** icon .
 - On the **Add Data Source** page, select **McAfee** in the **Data Source Vendor** field, then **Enterprise Security Manager (SEF)** in the **Data Source Model** field.
 - Complete the requested information, then click **OK**.
- 4 Add the event forwarding destination on the sending ESM.
 - Click the system on the system navigation tree, then click the **Properties** icon .
 - Click **Event Forwarding**, then click **Add**.
 - On the **Add Event Forwarding Destination** page, select **syslog (Standard Event Format)** in the **Format** field, then complete the remaining fields with the information for the ESM you are forwarding to, and click **OK**.

See also

Setting up event forwarding on page 278

Event forwarding agents on page 281

Configure event forwarding on page 279

Add event forwarding destinations on page 279

Enable or disable event forwarding on page 282

Modify settings for all event forwarding destinations on page 282

Add event forwarding filters on page 282

Edit event forwarding filter settings on page 283

Managing reports

Reports show data from events and flows managed on the ESM. You can design your own or run one of the predefined reports and send it in PDF, HTML, or CSV format.

Predefined reports

The predefined reports are divided into these categories:

- Compliance
- Executive
- McAfee ADM
- McAfee Database Activity Monitoring (DAM)
- McAfee DEM
- McAfee Event Reporter

They generate data based on events.

User-defined reports

When you create a report, you design the layout on the **Report Layout** editor by selecting the orientation, size, font, margins, and header and footer. You can also include components, setting them up to display the data as desired.

All layouts are saved and can be used for multiple reports. When you add a report, you are given the option to design a new layout, use an existing one as is, or use an existing one as a template and edit its features. You can also remove a report layout when it is no longer needed.

See also

Set start month for quarterly reports on page 285

Add reports on page 286

Add report layout on page 288

Include an image in PDFs and reports on page 291

Add a report condition on page 292

Display host names in a report on page 292

Set start month for quarterly reports

If you are running reports on a quarterly basis, you must define the first month of Quarter 1. Once this is defined and stored in the system table, reports run quarterly based on that start date.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM console, select **System Properties**, then click **Custom Settings**.
- 2 In the **Specify which month should be used** field, select the month.
- 3 Click **Apply** to save the setting.

See also

Managing reports on page 285

Add reports on page 286

Add report layout on page 288

Include an image in PDFs and reports on page 291


Add a report condition on page 292

Display host names in a report on page 292

Add reports

Add reports and run them regularly, at intervals you define, or run when you select them manually. You can select an existing report layout or create one using the **Report Layout** editor.

Task

- 1 From the dashboard, click  and select **Reports**.
- 2 Click **Add**, then define the settings on the **Add Report** page.
- 3 Click **Save**.

The report is added to the table on the **Reports** page and runs as defined in the **Condition** field.

Table 8-14 Option definitions

Option	Definition
Reports table	View the reports that are currently set up on the ESM.
Add	Define the settings for a new report and add it to the ESM.
Edit	Change the settings on an existing report.
Remove	Delete an existing report from the ESM.
Run Now	Run the selected report now.
Share	Share the selected reports with groups or users you choose.
Import	Import reports that have been previously exported.
Export	Export reports.
Enabled	Enable the report selected on the table.
Enable or Disable button	Enable or disable the reporting function. When it is disabled, none of the reports on the list generate.
Conditions	Manage the types of conditions that are available for reports.
Recipients	Manage the recipients defined on the ESM.
View	View the reports that are currently queued to run and cancel them if needed.
Files	Manage the generated reports files.

Table 8-15 Option definitions


Option	Definition
Report Name	Type a name for the report.
Description	Type a description of the information the report generates.
Condition	Select when you want this report to run from the list of options. To add a condition to the list of options, click Edit conditions .
Time Zone	Select the time zone that must be used to run the queries.
Date Format	Select the format to be used for the date.
Format	<p>Select the format you want the report generated in.</p> <ul style="list-style-type: none"> • If you are designing a new report, your options are PDF or HTML. • If you want to include a view in the report, select View PDF. • If you want to generate a CSV file of the results of the query, select Query CSV.
Email sent to users or groups	Select if you want the report to be sent to users or groups, then click Add Recipients to select them. If the report format is Report HTML or Query CSV , select whether you want the report sent as an attachment to the email or inline.
File saved to the ESM	<p>Select if you want the report saved in a file on the ESM. Prefix shows the default prefix for the name of the file, which you can change.</p> <p>Once the file has been generated, click Files on the Reports page to view the report.</p>
File saved to remote location	Select if you want the report saved in a remote location. Select the location from the drop-down list. If it is not listed, click manage locations... then add the remote location profile.
Choose an existing layout or create a new one	<p>If you selected PDF or HTML format, select an existing layout or create a new one. You can also manage the layouts.</p> <ul style="list-style-type: none"> • Choose and existing layout — Locate it on the list, then click it. • Add — Click to open the Report Layout editor and create a new layout. • Edit — Make changes to an existing layout. • Add Folder — Add a folder so you can organize your layouts. You can then add a new layout to the folder, drag-and-drop an existing layout into the folder, or add a subfolder. • Import — To import layouts, click and browse to the file you want to import. <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> If the layout that you are importing includes an image that currently exists on the ESM, Import Report Layouts opens informing you of this conflict and offering you the following choices:</p> <ul style="list-style-type: none"> • Keep Local — Keeps the image on the ESM and delete the image from the report layout. The image on the ESM is used for that layout. • Replace Local — Replaces the image on the ESM with the image in the report layout. Any layouts that currently use the image that you are deleting from the ESM now uses the image imported with the layout. • Rename — Renames the image in the report layout automatically and the layout is imported using the image with the new name. </div> <ul style="list-style-type: none"> • Export — Click to export layouts. • Include filter summary in report — Select to include a summary of the global and individual component filters defined for this report. The filters used are listed at the bottom of the report. This is useful if you want to know the limits defined for the data in the report.

Table 8-15 Option definitions *(continued)*

Option	Definition
Choose a view	If you selected View PDF as the format, select the view you want to include in the report from the drop-down list.
Choose a predefined query	If you selected Query CSV , select the predefined query.
Enter values to filter	Select the filters you want to apply to all the components in this report (see Query Filters page). You can use <code>contains</code> and <code>regex</code> filters in these fields (see <i>Description of contains and regex filters</i>).

See also

Managing reports on page 285

Set start month for quarterly reports on page 285

Add report layout on page 288

Include an image in PDFs and reports on page 291

Add a report condition on page 292

Display host names in a report on page 292

Add report layout

Design the layout for a report if the predefined layouts do not meet your needs.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Reports**.
- 2 Click **Add** to open the **Add Report** page, then complete sections 1, 2, and 3.
- 3 In section 4, select **Report PDF** or **Report HTML**.
- 4 In section 5, click **Add** to open the **Report Layout** editor.
- 5 Set up the layout to display the data generated by the report.

The layout is saved and can be used as is for other reports or as a template that you can edit.

Table 8-16 Option definitions

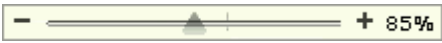



Option	Definition
	Slide the indicator back and forth to adjust the size of the editor page.
	Select to make the width of the editor page fit the width of the page.

Table 8-16 Option definitions (continued)

Option	Definition
Document Properties	<p>Define the basic formatting settings for the layout.</p> <ul style="list-style-type: none"> • Name and Description — Type a name for the layout and a description of its features. The name is required. • Orientation — Select whether you want the page to be portrait or landscape to print the report. • Size — The default size of the report page is 8.5 x 11. To change it, select the correct size on the drop-down list. The editor page reflects the change. • Default Font — Select the font type, size, and color for the text in the report. When you change it, the text on the editor page will reflect the change. You can also select if you want the text to be bold, italicized, underlined, centered, or aligned to the right of the page. • Margin — Select the margin for each edge of the report. • Header and Footer — Select whether you want a header and a footer on the report.
Header Properties	<p>Click in the header area on the editor page, then do the following in the Header Properties section:</p> <ul style="list-style-type: none"> • Report Name Font — Select the font you want to use for the layout name in the header. • Included Items — Select the items that you want to include in the header. If you change the font for these items, go to Document Properties. • Logo — Select if you want a logo in the header. If you do, select if you want it on the right or left side of the header, and click the link in the File field to select an image.
Footer Properties	<p>Click in the footer area on the editor page. In the Footer Properties section, select the items you want to include.</p>
Save	<p>Click to save the layout. You are notified if there are required settings that you neglected to define.</p>
Save As	<p>Save the layout with a new file name.</p>
Copy	<p>Click to copy the selected component in the layout. A clipboard icon, showing the type of component that was copied, is added on the left. You can then paste it in one of two ways:</p> <ul style="list-style-type: none"> • Drag-and-drop the icon to the location where you want to add the component. • Highlight a component in the layout and click Paste. The copied component inserts below the component you highlighted.

Table 8-16 Option definitions *(continued)*

Option	Definition
Components properties	<p>Drag and drop Text, Image, Table, Bar chart, Pie chart, or Distribution chart components on the editor page and define their settings as follows:</p> <ul style="list-style-type: none"> • Query Wizard — Define the query for the component you selected. • Font — Set the font type, size, and color; whether it should be bold, italicized, or underlined; and whether you want it left, center, or right justified. • Image — Select the image on the Image Selector page. • Title — Change the title if needed, set the font for the title, and select its justification. • Query — Make changes to the query if needed, and select the maximum number of results to display on the table. On Table, Bar Chart, or Pie Chart components, select Resolve IPs to Hostnames if you want the report to use DNS resolution for source and destination IP addresses. • Table Header — Set the font for the header row of the table. • Table — Set the font for the data in the table. • Border — Select whether you want a border around the text box, image, or table and, if so, its thickness and color. • Alternating Row Colors — If you want alternating rows of a table to be a different color, select the two colors you want to use. • Columns — Set the column names and formatting for each column in a table. • Subtotal Configuration — Select if you want to display subtotals on the table. • Other — On the pie chart, select if you want to show labels and a legend. • To adjust the size of a component, click the component on the editor page, click one of the yellow squares  that indicate the borders, then drag it to the size you want.
Page Break 	<p>Drag-and-drop to the location where you want to insert a page break. A bold black line indicates where the page break goes.</p>

See also*Managing reports on page 285**Set start month for quarterly reports on page 285**Add reports on page 286**Include an image in PDFs and reports on page 291**Add a report condition on page 292**Display host names in a report on page 292*

Add an image component to a report


Select an image to add to the body of a report as a component.

Before you begin

Ensure that the image file has already been added to the ESM or is in a location that is accessible from the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties** | **Reports** | **Add**, then complete sections 1 through 4.
- 2 In section 5, click **Add** to design a new report layout or select an existing layout and click **Edit**.
- 3 On the **Report Layout** page, drag and drop the **Image** icon  on the body section of the layout.
- 4 On the **Image Selector** page, click **Add** to upload a new image and select it, or select an image from the list.
- 5 Click **OK** to add the image to the report layout.

Include an image in PDFs and reports

You can set up the ESM so exported PDFs and printed reports include the image shown on the **Login** screen.

Before you begin

Add the image to the **Custom Settings** page.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Custom Settings**.
- 2 Select **Include image in exported PDF from Views or printed reports**.
- 3 Click **OK**.

Table 8-17 Option definitions

Option	Definition
Image Selector table	View the images that are on the ESM. Select one, then click OK .
Add	Add a new image to the ESM.
Rename	Change the name of an image that is currently on the ESM. The name of each image on the list must be unique.
Delete	Remove an image from the ESM.

See also

[Managing reports on page 285](#)

[Set start month for quarterly reports on page 285](#)

[Add reports on page 286](#)

[Add report layout on page 288](#)

[Add a report condition on page 292](#)

[Display host names in a report on page 292](#)

Add a report condition

Add conditions so they are available when setting up a report.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, then click **Reports**.
- 2 Click **Conditions**, then enter the information requested.
- 3 Click **OK** to save the settings.

This option appears on the list of available conditions when you select the condition for a report.

Table 8-18 Option definitions

Option	Definition
Conditions table	View the existing conditions.
Add	Specify the settings for a new condition.
Edit	Change the settings of an existing condition.
Remove	Delete an existing condition.

Table 8-19 Option definitions

Option	Definition
Name	Type a name for this condition.
Type	Select the frequency that you want the condition to trigger.
Notes	Type notes to explain what this condition does.
Properties	Define the details of the trigger time. The options are based on the type you selected.

See also

[Managing reports on page 285](#)

[Set start month for quarterly reports on page 285](#)

[Add reports on page 286](#)

[Add report layout on page 288](#)

[Include an image in PDFs and reports on page 291](#)


[Display host names in a report on page 292](#)

Display host names in a report

You can configure reports to use DNS resolution for source and destination IP addresses on reports.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Reports**, then click **Add** and fill in the requested information in sections 1 through 4.

- 3 In section 5, click **Add**, then drag-and-drop a **Table**, **Bar Chart**, or **Pie Chart** component and complete the **Query Wizard**.
- 4 In the **Query** section of the **Properties** pane on the **Report Layout** editor, select **Resolve IPs to Hostnames**.

In addition to appearing in the report, you can view the results of the DNS lookup on the **Hosts** table (**System Properties** | **Hosts**).

See also

[Managing reports on page 285](#)

[Set start month for quarterly reports on page 285](#)

[Add reports on page 286](#)

[Add report layout on page 288](#)

[Include an image in PDFs and reports on page 291](#)

[Add a report condition on page 292](#)

Description of *contains* and *regex* filters

The *contains* and *regex* filters provide you with wildcard capabilities on both index string data and non-indexed string data. These filters have syntax requirements.

These commands can be used in any field that allows text or string data. Most text fields are denoted by the case insensitivity icon **Aa** next to the filter field name. Other fields that allow *contains* do not have that icon. For a full list of fields, see the *Fields supporting the contains feature* section.

Syntax and Examples

The basic syntax for *contains* is `contains(somevalue)` and for *regex* is `regex(someregularexpression)`.

To make it case insensitive, click the icon **Aa** or include the `/i` regular expression notation, as in `regex(/somevalue/i)`. The search returns any value that contains *somevalue*, regardless of case.

The NOT **!** and OR **or** icons apply to the *regex* and *contains* values. If you want the results to show the values that do not contain some value, enter the value and click the NOT icon. If you want the results to show values that have one value or another, enter the values and click the OR icon.

Example #1 - A simple search

Indexed fields: `contains(stra), regex(stra)`

Non-indexed fields: `stra`

Result: Returns any string with `stra` , such as `administrator`, `gmestrad`, or `straub`.

Example #2 - An OR search

Indexed fields: `contains(admin,NGCP), regex((admin|NGCP))`

Non-indexed fields: `admin,NGCP`

Result: Returns any string within the field that contains `admin` or `NGCP`. The extra set of parentheses is required for the *regex* OR to function.

Example #3 - A search for special characters, such as in service accounts

A dollar sign:

Indexed fields: `contains ($), regex (\x24) or regex (\$)`

Non-indexed fields: `$`

Result: Either of these returns any string within the field that contains a `$`. Go to <http://www.asci.cl> for a list of HEX values for the characters.

With *regex*, if you try to use the `$` without scaling it, the result set returns empty. PCRE escape sequence is a better search method to use.

A percent sign:

Indexed fields: `contains (%), regex (\x25) or regex (\%)`

Non-indexed fields: `%`

A backslash:

Indexed fields: `contains (\), regex (\x5c) or regex (\\)`

Non-indexed fields: `\`

Dual back slashes

Indexed fields: `contains (\\), regex (\x5c\x5c) or regex (\\\\)`

Non-indexed fields: `\\`

In some cases, if you do not use the HEX value or the slash with *regex*, you may get an *Invalid Regular Expression (ER5-0015)* error.

Example #4 - Search using the * wildcard

Indexed fields: `contains (ad*)`

Non-indexed fields: `ad*`

Results: Returns any string that starts with `ad`, such as `administrator` and `address`.

Example #5 - Search using Regular Expression

These domains are from Microsoft DNS events.

```
regex(nitroguard\x28[3-4]\x29[com|info]+)
```

```
(3)www(10)nitroguard(3)com(0)
```

```
(3)www(10)nitroguard(4)info(0)
```

```
(3)www(10)nitroguard(3)gov(0)
```

```
(3)www(10)nitroguard(3)edu(0)
```

```
(3)www(10)nitroguard(7)oddball(0)
```

Results: This regular expression picks out a specific string. In this case, it's `nitroguard`, a 3- or 4-digit primary domain, and `com` or `info`. This *regex* matches the first two expressions but not the others. These are examples to show how *regex* can be used with the feature. Your expressions will be much different.

Caveats

- Using *regex* with values of less than three characters causes higher overhead and slower query performance. We suggest that all queries have more than three characters.
- This filter can't be used in correlation rules or alarms. The only exception is that it can be used in correlation rules with name/value custom types.
- Using *contains* or *regex* with NOT can cause higher overhead and slower query performance.

Bloom filter description

For information regarding a bloom filter, see http://en.wikipedia.org/wiki/Bloom_filter.

Fields supporting the *contains* and *regex* feature

Access_Resource	File_Operation_Succeeded	Referer
Application	File_Path	Registry_Key
Application_Protocol	File_Type	Registry_Value
Area	Filename	Request_Type
Authoritative_Answer	Forwarding_Status	Response_Code
Bcc	From	Return_Code
Caller_Process	From_Address	RTMP_Application
Catalog_Name	FTP_Command	Sensor_Name
Category	Host	Sensor_Type
Cc	HTTP_Req_Cookie	Sensor_UUID
Client_Version	HTTP_Req_Host	Session_Status
Command	HTTP_Req_Method	Signature_ID
Contact_Name	HTTP_Req_Referer	Signature_Name
Contact_Nickname	HTTP_Req_URL	SNMP_Error_Code
Cookie	HTTP_User_Agent	SNMP_Item
Creator_Name	Incomtin_ID	SNMP_Item_Type
Database_ID	Interface	SNMP_Operation
Database_Name	Interface_Dest	SNMP_Version
Datacenter_ID	Job_Name	Source_User
Datacenter_Name	Job_Type	Source_Context
DB2_Plan_Name	Language	Source_Logon_ID
Delivery_ID	Local_User_Name	Source_Network
Description	Logical_Unit_Name	Source_UserID
Destination_User	Logon_Type	Source_Zone
Destination_Directory	LPAR_DB2_Subsystem	SQL_Command
Destination_Filename	Mail_ID	SQL_Statement
Destination_Hostname	Mailbox	Step_Count
Destination_Logo_ID	Mainframe_Job_Name	Step_Name
Destination_Network	Malware_Insp_Action	Subject
Destination_UserID	Malware_Insp_Result	SWF_URL

Destination_Zone	Management_Server	Table_Name
Detection_Method	Message_ID	Target_Class
Device_Action	Message_Text	Target_Context
Direction	Method	Target_Process_Name
Directory	NTP_Client_Mode	TC_URL
DNS_Class	NTP_Opcode	Threat_Category
DNS_Name	NTP_Request	Threat_Handled
DNS_Type	NTP_Server_Mode	Threat_Name
Domain	Object	To
Event_Class	Object_Type	To_Address
External_Application	Operating_System	URL
External_DB2_Server	Policy_Name	URL_Category
External_Hostname	Privileged_User	User_Agent
External_SessionID	Process_Name	User_Nickname
Facility	Query_Response	Version
File_Operation	Reason	Virtual_Machine_ID
		Virtual_Machine_Name

These custom types can use `contains` and `regex`:

Views

- String
- Random string
- Name/value
- Hashed strings

Case management

- Notes
- Summary
- History

Working with ESM views

The ESM retrieves information about events, flows, assets, and vulnerabilities logged by a device. The information is correlated and inserted into the McAfee Security Event Aggregation and Correlation (MSEAC) engine.

Contents

- ▶ *Manage views*
- ▶ *View session details*
- ▶ *Filtering views*
- ▶ *Watchlists*
- ▶ *Flow views*
- ▶ ***Enhanced ELM search view***
- ▶ *View components*
- ▶ *Working with the Query Wizard*

Manage views

Managing views provides a quick way for you to copy, import, or export more than one view at a time. You can select the views to include on the list of views and assign permission for specific users or groups to access individual views.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 On the ESM console, click the **Manage Views** icon .
- 2 Perform any of the available options, then click **OK**.

Table 8-20 Option definitions

Option	Definition
Table	Select the views you want to display on the views list. If the folder is checked, all of its subfolders and views are selected. If the folder's checkbox is black, some of its subfolders and views are selected.
Add Folder	Create a custom folder to organize your views. Once it's added, you can drag and drop views into the folder.
Rename	Rename the selected folder or view. You can't rename read-only views.
Delete	Delete selected custom folders or views. You can't delete read-only views.
Copy	Copy a view and add it to the view list. Once you have copied a view, you can drag and drop it in another folder.
Share	Select the users or groups who should have permission to access and modify the selected views.
Import	Import view files to the ESM.
Export	Export a file of custom views so you can share it with another ESM or keep the file as a backup. Note that you cannot export read-only views.
Make this my default view	Select a specific view to become the default view in your view pane. To do so, click on the view and select this option.


View session details

You can view the details of an event with a session ID and save them to a csv file on the **Session Viewer**.

To have a session ID, an event must reside within a session. A session is the result of a connection between a source and destination. Events that are internal to the device or ESM do not have session IDs.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the view drop-down list, select the view that has the session you need to view.
- 2 Select the event, click the menu icon on the component title bar, then select **Event Drilldown | Events**.
- 3 Click the event, click the **Advanced Details** tab, then click the **View session data** icon  next to the **Session ID** field.

The **Session Viewer** opens, displaying the details of the session.

Filtering views

In the filters pane located on the main ESM console, you can set up filters to be applied to views. Any filters that are applied to a view are carried forward to the next view that is opened.

When you first log on to the ESM, the default filters pane includes the **Source User**, **Destination User**, **Source IP**, and **Destination IP** filter fields. You can add and delete filter fields, save filter sets, change the default set, manage all filters, and launch the string normalization manager.

An orange funnel icon appears in the upper-right corner of the view pane to alert you when filters are applied to the view. If you click this orange icon, all filters are cleared and the query is executed again.

Anywhere you have comma-separated filter values such as variables, global filters, local filters, normalized strings, or report filters, you must use quotes if they are not part of a watchlist. If the value is `Smith, John`, you must type `"Smith, John"`. If there are quotes in the value, you must enclose the quotes in quotes. If the value is `Smith, "Boy"John`, you must enter it as `"Smith, ""Boy""John"`.



You can use `contains` and `regex` filters (see [Description of contains and regex filters](#)).

See also

[Filter a view on page 298](#)

[Add UCF and Windows event ID filters on page 321](#)


[Select normalized IDs on page 299](#)

Filter a view

Filters help you view details about selected items on a view. If you enter filters and refresh the view, the data in the view reflects the filters you added.

Task


For details about product features, usage, and best practices, click **?** or **Help**.




- 1 On the ESM console, click the list of views, then select the view you want to filter.
- 2 In the **Filter** pane, fill in the fields with the data you want to filter on in one of these ways:
 - Type the filter information in the appropriate field. For example, to filter the current view to see only the data that has a source IP address of 161.122.15.13, type the IP address in the **Source IP** field.
 - Type a `contains` or `regex` filter (see [Description of contains and regex filters](#)).
 - Click the **Display filter list** icon  next to the field and select the variables or watchlists to filter on.
 - On the view, select the data you want to use as the filter, then click the field on the **Filter** pane. If the field is blank, it is auto-populated with the data you selected.



For **Average Severity**, use a colon (:) to enter a range. For example, 60:80 is a severity range of 60–80.

- 3 Do any of the following:

To...	Do this...
View data that matches more than one filter	Enter the values in each field.
View data that matches some filter values and excludes others	<ol style="list-style-type: none"> 1 Enter the filter values that you want to include and exclude. 2 Click the NOT icon  next to the fields you want to exclude.

To...	Do this...
View data that matches regular and OR filters	<ol style="list-style-type: none">1 Enter the filter values in the regular and the OR fields.2 Click the OR icon next to the fields that have the OR values. <p>The view includes the data that matches the values in the fields not marked OR, and matches either of the values in the fields marked OR.</p> <div> At least two fields must be marked OR for this filter to work.</div>
Make the filter values case-insensitive	Click the Case-insensitive icon  next to the appropriate filter field.
Replace normalized strings with their aliases	Click the string normalization icon  next to the appropriate filter field.

- 4 Click the **Run Query** icon .

The view is refreshed and the records matching the values you entered are displayed in the view. An orange filter icon appears in the upper-right corner of the view pane, indicating that the data in the view is a result of filters. If you click the icon, the filters are cleared and the view shows all data.

Table 8-21 Option definitions

Option	Definition
Table	View the filter sets that were added to the ESM (see <i>Filters pane</i>), as well as all possible filters. You can organize this list by adding folders and dropping filter sets in them.
Add Folder	Add a new folder to help you organize the filters. Once added, you can drag and drop filter sets to the new folder.
Add Filter Set, Edit Filter Set	Add a new filter set to the list of possible filters or edit an existing one.
Rename	Change the name of the selected folder or filter set.
Delete	Delete a folder or filter from the list.
Copy	Copy an existing filter. After you rename it, it is added to the bottom of the list. You can then use it as a template and make changes to its settings, using Edit Filter Set .
Share	Share the selected folders or filter sets with other users or groups on the system.

See also

[Filtering views on page 298](#)

[Add UCF and Windows event ID filters on page 321](#)


[Select normalized IDs on page 299](#)

Select normalized IDs

When you are creating a new view or adding a filter to a view, you can select to filter the data using Normalized IDs.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM console, do one of the following:
 - If you are creating a new view, click **Filters** on the second page of the **Query Wizard** (see *Define view or report component settings*).
 - If you are adding filters to a view, select the view to which you want to add them. The **Filters** pane is on the right of the screen.
- 2 Locate the **Normalized ID** field, then click the **Filters** icon .
- 3 Select the IDs, then click **OK**.

The ID numbers selected are added to the **Normalized ID** field.

See also

[Filtering views on page 298](#)

[Filter a view on page 298](#)

[Add UCF and Windows event ID filters on page 321](#)

View event time

View the exact time that an event was inserted into the Receiver's database.


Before you begin

You must have these permissions:

- **View Data** to get events and view the event time
- **View Management** to create a view
- **Event Management** to change events

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 On the ESM console, add an events table view that includes the **Device Time** field.
 - a On the View pane toolbar, click the **Create New View** icon .
 - b On the **View Editing Toolbar**, click and drag the **Table** component.
 - c On the **Query Wizard**, click **Next**, then click **Fields**.
 - d Click **Device Time** in the list on the left, and move it to the list on the right.
 - e On the **Fields** page, click **OK**, then click **Finish**.
 - f On the **View Editing Toolbar**, click **Save As**, type the name for the view, then click **OK**.
 - g Close the **View Editing Toolbar**.

The view is added to the drop-down list of views.

- 2 View the **Device Time** in one of these ways.



If you send an event to remedy (see *Send a remedy email*), the device time for that event is lost.

- View the **Device Time** column in the event table of the view you added.
- Click the **View Data Details** icon  in the toolbar at the bottom of the table, click the **Advanced Details** tab, then view the **Device Time** field.

Watchlists

A *watchlist* is a grouping of a specific type of information that can be used as a filter or as an alarm condition. It can be global or shared to a specific user or group and can be static or dynamic. A *static watchlist* consists of specific values that you enter or import. A *dynamic watchlist* consists of values that result from a regular expression or string search criteria that you define.

A watchlist can include a maximum of 1,000,000 values. The list of values on the **Add Watchlist** or **Edit Watchlist** pages can display up to 25,000 values. If there are more, you are informed that there are too many values to display. If you want to edit a watchlist by adding values that increase the total number to more than 25,000, you must export the existing list to a local file, add the new values, then import the new list.

You can set up the values on a static watchlist to expire. Each value is time-stamped and expires when the duration specified is reached, unless it refreshes. Values refresh if an alarm triggers and adds them to the watchlist. You can refresh the values set to expire by appending them to the list using the **Append to watchlist** option on the menu of a view component (see *Component menu options*).

You can set up the values on a dynamic watchlist to update periodically. The source is queried using the data given and the values are refreshed at the specified time.

See also

[Add watchlists on page 301](#)

[McAfee GTI watchlist on page 304](#)


[Create a watchlist of threat or IOC feeds from the Internet on page 304](#)

[Add a Hadoop HBase watchlist on page 305](#)

Add watchlists

Use watchlists as filters or alarm conditions.

Task

- 1 Access the **Watchlists** page in one of these ways:
 - From the dashboard, click  and select **Watchlists**.
 - On the system navigation tree, click **System Properties**, then click **Watchlists**.
 - On an **Internal Event Match** alarm, click the **Actions** tab, select **Update Watchlist**, then click **Configure**.

The **Watchlists** table shows all watchlists on the system.





GTI Malicious IPs and **GTI Suspicious IPs** appear on the table, but don't contain data unless you purchased a McAfee GTI license from McAfee. To purchase a license, contact your McAfee Sales Engineer or McAfee support.

- 2 Click **Add** or **Add New Watchlist**, then fill in the information requested.
- 3 Click **OK** to add the new watchlist to the **Watchlists** table.

Table 8-22 Option definitions

Tab	Option	Definition
Main	Name	Type a name for the watchlist.
	Static or Dynamic	Select whether the watchlist is static or dynamic. Static watchlists consist of values you specify. Dynamic watchlists consist of values that result from regular expression or string search criteria you define.
	Values Expire	(Static) Select to time stamp each value on the watchlist so it expires when specified. When the duration you specify is reached, it expires unless it refreshes. Values refresh if an alarm triggers and adds them to the watchlist. To refresh the values set to expire, append them to the list using Append to watchlist on the menu of a view component.
	Duration	(Static) Select the amount of time that you want the values to be maintained. The range is from one hour to 365 days. When that time passes, the value is deleted from the watchlist, unless it is refreshed.
	Enable automatic updates	(Dynamic) Select if you want this list to be updated automatically at a time you specify.
	Update	Select how often the search is updated. The existing values list is replaced every time the search runs.
Source	Select the search source type. The remaining fields on the page vary based on the type you select. Most of them are self-explanatory.	
	ESM Strings	Searches the <i>StringMap</i> table, which contains strings found in events. Enter the regular expression or string search criteria in the Search field. Searches are case-sensitive by default. To perform a case-insensitive search, surround your search string or regular expression with forward slashes followed by <i>i</i> , such as <i>/Exploit/i</i> .
	ESM Rule Names	Searches the rule messages from the Rule table, which contain a short description of the rule. Enter the regular expression or string search criteria in the Search field. Searches are case-sensitive by default. To perform a case-insensitive search, surround your search string or regular expression with forward slashes followed by <i>i</i> , such as <i>/Exploit/i</i> .
	HTTP/HTTPS	Fill in these fields: <ul style="list-style-type: none"> • Authentication — Select Basic if the website requires a user name and password to log on. Default setting is None. • Ignore Invalid Certificates — If the website you are trying to search is an https URL, select this option to ignore invalid SSL certificates. • Method — If the website that you want to search requires a post content or argument, select POST. Default setting is GET.
	Active Response	Fill in these fields: <ul style="list-style-type: none"> • Collector — Select the collector that you want to use to pull data. • Value — Select the column of retrieved data that you want to include in the watchlist. • Or or And — Select whether you want all the filters to be applied to the data (And) or either of the filters applied (Or). This only applies when you have two or more filters. • Filters — Filters you want to apply to the search. • Add Filter — Click to add another filter line. You can have a maximum of five filters. <p>To delete a filter, click the delete icon to the right of the filter.</p>

Table 8-22 Option definitions (continued)

Tab	Option	Definition
Parsing	Raw data	When HTTP/HTTPS is selected as the source type, view the first 200 lines of the source code in the URL field on the Source tab. It is only a preview of the website, but is enough for you to write a regular expression to match. A Run Now or scheduled update of the watchlist includes all matches from your regular expression search. This feature supports RE2 syntax regular expressions, such as <code>(\d{1,3}\.){1,3}\.d{1,3}</code> .
	Header lines to skip	Typically, an Internet site has header code that you don't have to search. Specify how many lines from the top of the site you want to skip so that the search doesn't include header data.
	New line delimiter	Type what is used on the site to separate the values. This field has a default of <code>\n</code> , which indicates that a new line is the delimiter. The other most common delimiter is a comma.
	Ignore Expression	Type a regular expression that would remove any unwanted values from the results of your regular expression search.
	Regular Expression	(Required) Type the logic used to find a match and extract the values from the site. Use this to create an expression that matches on a list of known malicious IP addresses or MD5 sums listed on a site.
	Matching Group	If your regular expression contains multiple match groups, select a group from this drop-down list.
Values	Type	<p>Select a type that assigns the search results to a field type. This type allows the watchlist to be used throughout the system, such as for filters or alarms. You can change this setting on an existing watchlist. If it has less than 25,000 values, ESM validates that the old and new types are compatible and returns an error if they aren't. If it has more than 25,000 values, you must validate compatibility.</p> <div>  <p>If this is a dynamic watchlist and you select String as the source, the application does not filter the search by the type you select. Instead, the search returns all matching strings.</p> </div>
	Values	<p>For a static watchlist, import a file of values in new-line-separated format or type the values, one value per line.</p> <div>  <p>Both static and dynamic watchlists are limited to a maximum number of 1,000,000 values.</p> </div> <p>For a dynamic watchlist, the values table fills with values every time a search runs. If there are more than 25,000 values in the watchlist, the Values field states that there are more values than can be displayed.</p> <p>User name identifies who can access the database. For LDAP, the user name must be a fully qualified domain name without spaces, such as:</p> <pre>uid=bob,ou=Users,dc=example,dc=com</pre> <p>or</p> <pre>administrator@company.com</pre>
	Clear Values	Click if you want to delete all items on the Values list.
	Import	Click to add imported values to the Values list. If there are more than 25,000 imported values, a message indicates that not all imported values can be displayed.
	Export	Click if you want to export the list of values.
	Run Now	Click if you want to run the query now. The results populate the Values box.

See also

[Watchlists on page 301](#)

[McAfee GTI watchlist on page 304](#)

[Create a watchlist of threat or IOC feeds from the Internet on page 304](#)

[Add a Hadoop HBase watchlist on page 305](#)

Update watchlist with alarm data

You can set an alarm to update a watchlist by adding or removing triggering event data generated by a maximum of 10 alarm events per triggered alarm.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, click **System Properties**, then click **Alarms | Add**.
- 2 On the **Alarms Settings** page, click the **Condition** tab, then select **Internal Event Match** or **Field Match** in the **Type** field.
- 3 Click the **Actions** tab, select **Update Watchlist**, then click **Configure**.
- 4 Select the action to take, the field from the triggering event to append or remove, and the watchlist to update, then click **OK**.

McAfee GTI watchlist

McAfee GTI watchlists contain more than 130 million suspicious and malicious IP addresses and their severities, gathered by McAfee. These watchlists can be used to trigger alarms, to filter data in reports and views, as a filter in rule correlation, and as a scoring source for a Risk Correlation Manager on an ACE.

To add the data from the lists to your system, you must purchase a McAfee GTI license from McAfee. Once you do, the lists are added to your system the next time you download rules. This process can take several hours due to the size of the database.



You must have an Internet connection to download the lists. They can't be downloaded off line.

These lists cannot be viewed or edited, but the **Watchlists** table (**System Properties | Watchlists**) indicates whether the list is *active* (contains values) or *inactive* (does not contain values).

To purchase the McAfee GTI license, contact your McAfee Sales Engineer or McAfee Support.

See also

[Watchlists on page 301](#)

[Add watchlists on page 301](#)

[Create a watchlist of threat or IOC feeds from the Internet on page 304](#)

[Add a Hadoop HBase watchlist on page 305](#)


Create a watchlist of threat or IOC feeds from the Internet

You can create a watchlist that can be refreshed periodically to automatically pull threat or Indicator of Compromise (IOC) feeds from the Internet.

On this watchlist, you can preview the data to be retrieved through the HTTP request, as well as add regular expressions to filter this data.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click the system, then click the **Properties** icon .
- 2 Click **Watchlists**, then click **Add**.
- 3 Complete the **Main** tab, selecting **Dynamic**.
- 4 Click the **Source** tab, select **HTTP/HTTPS** in the **Type** field.
- 5 Complete the information requested on the **Source**, **Parsing**, and **Values** tabs.



The **Raw data** field on the **Parsing** tab is populated with the first 200 lines of the html source code. It is just a preview of the web site, but is enough for you to write a regular expression to match on. A **Run Now** or scheduled update of the watchlist includes all matches from your regular expression search. This feature supports RE2 syntax regular expressions, such as `(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})` to match on an IP address.

See also

[Watchlists on page 301](#)

[Add watchlists on page 301](#)

[McAfee GTI watchlist on page 304](#)


[Add a Hadoop HBase watchlist on page 305](#)

Add a Hadoop HBase watchlist

Add a watchlist using Hadoop HBase as the source.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system, click the **Properties** icon , then click **Watchlists**.
- 2 On the **Main** tab of the **Add Watchlist** wizard, select **Dynamic**, enter the information requested, then click the **Source** tab.
- 3 Select **Hadoop HBase (REST)** in the **Types** field, then type the host name, port, and name of the table.

- 4 On the **Query** tab, fill in the lookup column and query information:
 - a Format **Lookup Column** as `columnFamily:columnName`
 - b Populate the query with a scanner filter, where the values are Base64 encoded. For example:

```
<Scanner batch="1024">
<filter>
{
  "type": "SingleColumnValueFilter",
  "op": "EQUAL",
  "family": " ZW1wbG95ZWVJbmZv",
  "qualifier": "dXNlcm5hbWU=",
  "latestVersion": true,
  "comparator": {
    "type": "BinaryComparator",
    "value": "c2NhcGVnb2F0"
  }
}
</filter>
</Scanner>
```

- 5 Click the **Values** tab, select the value type, then click the **Run Now** button.

See also

[Watchlists on page 301](#)

[Add watchlists on page 301](#)

[McAfee GTI watchlist on page 304](#)

[Create a watchlist of threat or IOC feeds from the Internet on page 304](#)

Flow views

A *flow* is a record of a connection made through the device. When flow analysis is enabled, data is recorded about each flow, or connection.

Flows have source and destination IP addresses, ports, Mac addresses, a protocol, and a first and last time (indicating duration between the start and finish of the connection).

Because flows are not an indication of anomalous or malicious traffic, there are more flows than events. A flow is not associated with a rule signature (SigID) like an event. Flows are not associated with event actions such as Alert, Drop, and Reject.

Certain data is unique to flows, including source and destination bytes and source and destination packets. *Source bytes* and *packets* indicate the number of bytes and packets transmitted by the flow's source. The *destination bytes* and *packets* indicate the number of bytes and packets transmitted by the flow's destination. Flows have direction: an *inbound flow* is defined as a flow that originates from outside the HOME_NET. An *outbound flow* originates from inside the HOME_NET.

To view flow data, you must enable your system to log flow data. You can then view flows on the **Flow Analysis** view.

See also

[Enhanced ELM search view on page 307](#)

[Perform an enhanced ELM search on page 307](#)

Enhanced ELM search view

The **Enhanced ELM Search** view is available when there is at least one ELM device on the system. It allows you to perform more detailed searches and provides real-time tracking of search progress and results when you perform a search of logs on one or more ELM.

This view takes advantage of the archive statistical reporting capabilities on the ELM to provide real-time information about the amount of data that must be searched, allowing you to limit the query to minimize the number of files to be searched.

While the search is processing, the graphs show the estimated results:

- **Results Time Distribution** graph — Displays the estimates and results based on a time distribution. The bottom axis changes depending on what is selected in the time frame drop-down list.
- **Data Source Results** graph — Displays the estimates and results per data source based on the data sources of the devices selected on the system navigation tree.
- **Device Type Results** graph — Displays the estimates and results per device type based on the devices selected on the system navigation tree.

These graphs are populated before the searching begins and are updated as results are found. You can select one or more bars on the **Data Source Results** or **Device Type Results** graphs, or highlight a section of the **Results Time Distribution** graph. Click **Apply Filters** to narrow the search once the results have started coming in. This allows you to drill down to the search results, and to limit the amount of data that needs to be searched. When the search is finished, these graphs display the actual results.

See also

[Flow views on page 306](#)

[Perform an enhanced ELM search on page 307](#)

Perform an enhanced ELM search

Search the logs on one or more ELM devices for information that you define.

Task





For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the view pane, select **Enhanced ELM search** from the drop-down list.
- 2 If there is more than one ELM device on the system, select the devices to search from the drop-down list next to the text field.
- 3 Type a normal text search or regular expression in the text field.
- 4 If you want a time frame other than **Current Day**, select it on the drop-down list.
- 5 On the system navigation tree, select the devices that you want to search.
- 6 If needed, select one or more of these options:
 - **Case Insensitive** — Makes the search case-insensitive.
 - **Regular Expression** — Treats the term in the search field as a regular expression.
 - **Does NOT Contain Search Term** — Returns matches that don't contain the term in the search field.

7 Click **Search**.

The results are displayed in the **Search Results** section of the view.

8 Do any of the following during the search or after it is completed.

Option	Definition
Save search 	Save the results of this search, even if you navigate away from the view. Saved searches can be viewed on the ELM Properties Data page.
Download search results file 	Download the results to the location you designate.
Copy selected items to clipboard 	Copy the items you select to the clipboard, so you can paste them into a document.
View data details 	Show details for any logs that you select in the Search Results table.

See also

[Flow views](#) on page 306

[Enhanced ELM search view](#) on page 307

View components

Create custom views to display event, flow, asset, and vulnerabilities data in a way that is most useful to you.


Each view consists of components you select on the **View Editing Toolbar** and set up to display the data. When you select one, the **Query Wizard** opens, allowing you to define details about the data displayed in the component.

Look around an event

From the **Event Analysis** view, you can look for events that match one or more of the fields in the event in the time frame you select.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 On the ESM console, click the views list, then select **Event Views | Event Analysis**.
- 2 Click an event, click the menu icon , then click **Look Around**.
- 3 Select the number of minutes before and after the time of the event that you want the system to search for a match.
- 4 Click **Select filter**, select the field that you want the search to match on, then type the value.

The results are displayed on the **Look Around Results** view.



If you leave this view, then want to return to it later, click **Last Look Around** on the **Event Analysis** menu.

Table 8-23 Option definitions

Option	Definition
Time frame	Select the number of minutes before and after the time of the selected event that you want the system to search for a match.
Select filter	Select the field type and enter the value that you want to search for. When you fill in one field, another field is added, allowing you to add as many filters as needed.
	Click to delete one of the filter fields.

View the IP address details of an event

If you have a McAfee® Global Threat Intelligence™ (McAfee GTI) license from McAfee, you have access to the new **Threat Details** tab when you perform an **IP Address Details** lookup. When you select this option, details about the IP address are returned, including risk severity and geolocation data.

Before you begin


Purchase a McAfee GTI license (see *McAfee GTIWatchlist*).



If your McAfee GTI license has expired, contact your McAfee Sales Engineer or McAfee support.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the ESM console, select a view that includes a table component such as **Event Views** | **Event Analysis**.
- 2 Click an IP address, click the menu icon  on any component that has an IP address, then click **IP Address Details**.

The **Threat Details** tab lists the data for the selected IP address. You can copy the data to the system clipboard.




The **IP Address Details** option has replaced the **WHOIS Lookup** option on the context menu. However, the **IP Address Details** page includes a **WHOIS Lookup** tab that shows this information.

Send a remedy email

If you set up a remedy system, you can send an email message to notify the system of an event that requires a remedy. When you follow this process, you receive a remedy case number to add to the event record.

For details about product features, usage, and best practices, click ? or **Help**.

Task


- 1 On an event view, highlight the event that requires remedial action.
- 2 Click the **Assign events to a case or Remedy** icon , then select **Send event to Remedy**.
- 3 Add the **Prefix**, **Keyword**, and **Enterprise User ID**.
- 4 (Optional) Add information under **Details**, which contains information generated by the system regarding the event.
- 5 Click **Send**.

Perform a WHOIS or ASN lookup

On a table component, you can perform a WHOIS lookup to find information about a source or destination IP address. **ASN Lookup**, available on ASN query on a bar chart and any flow record on a table that has ASN data, retrieves a WHOIS record using the ASN identifier.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Select an IP address or flow record with ASN data listed on a table component, or an ASN query bar on a bar chart component.
- 2 Click the menu , then select **IP Address Details** or **ASN Lookup**.

- 3 To look up another IP address or identifier:
 - On the **WHOIS** tab page, select an IP address from the list and enter the host name.
 - On the **ASN Lookup** page, type in the numbers or select one from the list.

Table 8-24 Option definitions

Option	Definition
Hostname	If you have the host name for the IP address, type it.
IP Address	If you typed a host name, the IP address is in this field. If you don't have a host name, type the IP address.
Look up	Click to start the DNS look up to retrieve the WHOIS record.
WHOIS Record	View the results of the lookup.

See also

[Add remedy case ID to event record on page 310](#)

[Export a component on page 310](#)

Add remedy case ID to event record

When you send an event email to the remedy system, you receive a Case ID number. You can add it to the event record for reference purposes.

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 Highlight the event on the **Event Analysis** view, then click the menu .
- 2 Select **Set Remedy Case ID**, type the number, and click **OK**.

Table 8-25 Option definitions

Option	Definition
Event ID	If you accessed this page by selecting an event on a view, the ID number of the event will be in this field.
Remedy Case ID	Type the ID you received (see <i>Send a remedy email</i>).

See also

[Perform a WHOIS or ASN lookup on page 309](#)

[Export a component on page 310](#)


Export a component

You can export the data on an ESM view component. Chart components can be exported in text or PDF formats and table components in common separated values (CSV) or HTML.

When exporting the current page of a chart, distribution, or table component on a view, the exported data matches exactly what you see when you initiate the export. If you export more than one page, the query runs again as it exports the data, so it might be different from what you see on the component.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On a view, click the menu  for the component you want to export, then click **Export**.
- 2 Select one of the following formats:
 - **Text** — Export the data in text format.
 - **PDF** — Export the data and an image.
 - **Image to PDF** — Export only the image.
 - **CSV** — Export a list in comma-delimited format.
 - **HTML** — Export the data in a table.
- 3 On the **Export** page, specify the data that you want to export.
 - If you selected **Text** or **PDF**, you can export the current page of data or a maximum number of pages starting at page 1.
 - If you selected **Image to PDF**, the image is generated.
 - If you selected **CSV** or **HTML**, you can export the selected items, the current page of data, or a maximum number of pages, starting at page 1.
- 4 Click **OK**

The export file is generated and you are prompted to download the resulting file.

Table 8-26 Option definitions

Option	Definition
Just the selected items	Highlight the items to export, then select this option.
Just the current page	Export the items you can currently see in the view. The exported data matches exactly what you see when you initiate the export.
Up to a maximum number of pages	Select the maximum number of pages to export. The query runs again as it exports the data, so it might be different from what you see on the component.

See also

[Perform a WHOIS or ASN lookup on page 309](#)

[Add remedy case ID to event record on page 310](#)

Working with the Query Wizard

Each report or view on the ESM gathers data based on the query settings for each component.

When adding or editing a view or report, define the query settings for each component on the **Query Wizard** by selecting the query type, the query, the fields to include, and the filters to use. All the queries on the system, both predefined and custom, are listed on the wizard so you can select the data you want gathered by the component. You can also edit or remove queries, and copy an existing query to use as a template to set up a new query.



See also[Manage queries on page 312](#)[Bind dashboard widgets on page 229](#)[Comparing values on page 314](#)[Compare graph values on page 314](#)[Set up stacked distribution for views and reports on page 315](#)**Manage queries**

The ESM comes with predefined queries that you can select on the **Query Wizard** when adding or editing a report or view. You can edit some of the settings on these queries and you can add and remove custom queries.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 Do one of the following to access the **Query Wizard**.


To...	Do this...
Add a view	<ol style="list-style-type: none"> 1 Click the Create New View icon  on the view toolbar. 2 Drag and drop a component from the View Editing Toolbar to the view pane. <p>The Query Wizard opens.</p>
Edit an existing view	<ol style="list-style-type: none"> 1 Select the view you want to edit. 2 Click the Edit Current View icon  on the view toolbar. 3 Click the component that you want to edit. 4 Click Edit Query in the Properties pane. <p>The Query Wizard opens on the second page.</p>
Design the layout for a new report	<ol style="list-style-type: none"> 1 On System Properties, click Reports. 2 Click Add. 3 In section 5 of the Add Report page, click Add. 4 Drag and drop a component in the report layout section. <p>The Query Wizard opens.</p>
Edit the layout on an existing report	<ol style="list-style-type: none"> 1 On System Properties, click Reports. 2 Select the report to edit, then click Edit. 3 In section 5 of the Edit Report page, select an existing layout, then click Edit. 4 Click the component in the report layout section, then click Edit Query in the Properties section. <p>The Query Wizard opens on the second page.</p>

- 2 On the **Query Wizard**, do one of the following:

To do this...	Do this...
Add a query	<ol style="list-style-type: none"> 1 Select the query that you want to use as a template, then click Copy. 2 Type the name for the new query, then click OK. 3 On the list of queries, click the one that you just added, then click Next. 4 On the second page of the wizard, change the settings by clicking the buttons.
Edit a custom query	<ol style="list-style-type: none"> 1 Select the custom query that you want to edit, then click Edit. 2 On the second page of the wizard, change the settings by clicking the buttons.
Remove a custom query	Select the custom query that you want to remove, then click Remove .

3 Click **Finish**.

Table 8-27 Option definitions

Option	Definition
Query type	<p>Lists the types of queries that are available for the component you selected. It can include event, flow, miscellaneous, assets and vulnerabilities, and risk status.</p> <div>  Stacking is not available for Collection Rate or Average (for example, Avg Severity Per Alert or Avg Duration Per Flow) distribution queries . </div>
Queries	Lists the predefined and custom queries available for the type you selected. If you added custom types, they are included. You can edit, copy, and remove custom queries on this list.
Fields	<p>Shows the information that is included on the component. You can change these settings for a table component on the second page of the wizard.</p> <ol style="list-style-type: none"> 1 Click Fields. 2 On Query Fields, move the field you want to include in the list on the right, using the side-to-side arrows. 3 Put the fields in the order you want them to appear on the table, using the up and down arrows, then click OK.
Filters	Shows the filter values set for the query. You can change these settings for any query on the second page of the wizard.
Sort on	Shows the order the results of the query are listed. You can change these settings for most queries on the second page of the wizard.
Compare	Provides a way for you to compare the number of distinct values of any of the existing filter files against the time distribution for events and flows. It is only available on a distribution component (see <i>Comparing values</i> and <i>Compare graph values</i>).
Stacking	Allows you to stack bar, line, and area charts on a distribution component so you can see the distribution of events related to a specific field.
CIDR Mask	Allows you to add a CIDR mask, which is used to group IP addresses. This option is only available when you select a Source IP or Destination IP query on a Bar Chart component.
Levels	Allows you to specify the normalized ID mask level for the query (see <i>Select normalized IDs</i>). It is available on pie chart, bar chart, and list components when you select the Normalized Event Summary query.

See also*Working with the Query Wizard on page 311**Bind dashboard widgets on page 229**Comparing values on page 314**Compare graph values on page 314**Set up stacked distribution for views and reports on page 315***Comparing values**

Distribution graphs have an option that allows you to overlay an additional variable on top of the current graph.

In this way, two values can be compared to easily show the relationships, for example, between total events and average severity. This feature provides valuable data comparisons over time, at a glance. This feature is also useful for saving screen real-estate when building large views, by combining results onto a single distribution graph.

The comparison is limited to the same type as the selected query. For example, if an event query is selected, you can compare with the fields from the event table only, not the flow or assets and vulnerabilities table.




When you apply the query parameters to the distribution chart, it runs its query as normal. If the comparison field is enabled, a secondary query is run for the data at the same time. The distribution component displays the data for both data sets on the same graph, but uses two separate vertical axes. If you change the chart type (lower-right corner of component), both sets of data continue to display.

See also*Working with the Query Wizard on page 311**Manage queries on page 312**Bind dashboard widgets on page 229**Compare graph values on page 314**Set up stacked distribution for views and reports on page 315***Compare graph values**

You can compare the data in a distribution graph with a variable you select.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 Select the **Create new view** icon  or the **Edit current view** icon .
- 2 Click the **Distribution** icon , then drag and drop it on the view to open the **Query Wizard**.
- 3 Select the query type and the query, then click **Next**.
- 4 Click **Compare**, then select the field that you want to compare to the query you selected.
- 5 Click **OK**, then click **Finish**.
- 6 Move the component to the correct location on the view, then:
 - Click **Save** if you are adding the component to an existing view.
 - Click **Save As** and add the name for the view if you are creating a new view.

See also

[Working with the Query Wizard on page 311](#)

[Manage queries on page 312](#)

[Bind dashboard widgets on page 229](#)

[Comparing values on page 314](#)

[Set up stacked distribution for views and reports on page 315](#)

Set up stacked distribution for views and reports

Set up the distribution component on a view or report so that you can see the distribution of events related to a specific field.

You can select the field to stack by when you add the component to a view or report. When you access the view, you can change the settings, set the interval, and set the chart type and details.



You can't use the **Stacking** and **Compare** features in the same query.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 Drag and drop the **Distribution** component on a view (see *Add a custom view*) or a report (see *Add report layout*), then select the type of query.



Stacking is not available for **Collection Rate** or **Average** (for example, **Avg Severity Per Alert** or **Avg Duration Per Flow**) distribution queries.

- 2 On the second page of the **Query Wizard**, click **Stacking**, then select the options.
- 3 Click **OK** on the **Stacking Options** page and **Finish** on the **Query Wizard**.


The view is added. You can change the settings, and set the interval and chart type by clicking the **Chart Options** icon .

Table 8-28 Option definitions

Option	Definition
Field to group bar segments by	Select the field to record the data for.
Number of bar segments per bar	Select the number of separate items you want to see data for in the bars. For example, if you select Signature ID and 10 , each bar shows the 10 signature IDs received most often during the time period you select.
Show 'Other' value	Select whether you want the component to include an Other bar. Using the above example, it would show the number of other signature IDs received.
Show Legend	On a view, select whether you want the legend to be included. In a report, it is always included.
Time Interval Options	(Only available when you click Chart Options icon on the view) Select the interval of time that you want each bar on the chart to represent.
Chart Options	(Only available when you click Chart Options icon on the view) Select the type of chart, then select whether you want to show the data details section on the view.

See also

[Working with the Query Wizard on page 311](#)

[Manage queries on page 312](#)

[Bind dashboard widgets on page 229](#)

[Comparing values on page 314](#)

[Compare graph values on page 314](#)

Change the default view

The **Default Summary** view appears in the view pane by default when you first log on to the ESM console. You can change this default view to any of the predefined or custom views on the ESM.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM console navigation bar, click **Options**, then select **Views**.
- 2 On the **Default System View** drop-down list, select the new default view, then click **OK**.

String normalization

Use string normalization to set up a string value that can be associated with alias values and to import or export a .csv file of string normalization values.

This enables you to filter the string and its aliases by selecting the string normalization icon next to the appropriate field in the **Filter** pane. In the case of the John Doe user name string, you define a string normalization file where the primary string is John Doe and its aliases are, for example, DoeJohn, JDoe, john.doe@gmail.com, and JohnD. You can then enter John Doe in the **User_Nickname** filter field, select the string normalization filter icon next to the field, and refresh the query. The resulting view displays all events associated with John Doe and his aliases, enabling you to check for login inconsistencies where source IPs match but user names do not. This feature can also assist you in meeting regulations requiring that you report privileged user activity.

See also

[Manage string normalization files on page 316](#)

[Create a string normalization file to import on page 317](#)

Manage string normalization files

Before you can use a string normalization file, you must add it to the ESM.

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 On the **Filters** pane, click the **Launch string normalization manager** icon .
- 2 Perform any of the available actions, then click **Close**.

Table 8-29 Option definitions

Option	Definition
Add	Click to add a normalized string.
Edit	Change the selected normalized string.
Remove	Delete the selected normalized string.
Import	Import a .csv file of aliases to the string normalization list (see <i>Create a file to import</i>).
Export	Click to export the selected items on the string normalization list. This file does not include commands. If you want to import this file, you must add a command to each alias in the file.

See also

[String normalization on page 316](#)

[Create a string normalization file to import on page 317](#)

Create a string normalization file to import

If you create a .csv file of aliases, you can import it on the **String Normalization** page so that it can be used as a filter.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 In a text or spreadsheet program, type the aliases using this format:

```
command, primary string, alias
```

Possible commands are `add`, `modify`, and `delete`.

- 2 Save it as a .CSV file, then import the file.

See also

[String normalization on page 316](#)

[Manage string normalization files on page 316](#)

Custom type filters

Custom type fields can be used as filters for views and reports and to create custom rules, to define and then access data that is most relevant to you.

The data generated by these custom type fields can be viewed in the **Details** section of the **Event Analysis** or **Flow Analysis** view.

You can add, edit, or remove custom types as well as export and import them. Use the **Edit** page to change the name. If it is a custom data type, you can also change the subtype settings.

Export or import custom types

When you export custom types, all are exported to the location that you select. When you import a file of custom types, the imported data replaces the current custom types on the system.

Custom queries

When you are setting up a custom query for a view, the predefined custom types appear as options when you are selecting the fields for the query. If you add a custom type as a field in the query, it acts as a filter. If the information that you are querying has no data for that custom type, the query table returns with no results. To avoid this, select the user field (Custom Field 1 through 10 in the **Event Field** column of the table) that returns the results that you need instead of using the custom type.

For example, let's say you want the query results to include source user data, if there is any. If you select **Source User** as a query field, it acts as a filter and, if the information you are querying has no source user data, the query returns no results. However, if you select User Field 7, which is designated as the user field for source user, it doesn't act as a filter and appears as a column in the table of results. If there is source user data, it appears in this column. If there isn't data for this field, the User Field 7 column is blank but other columns are populated.

Custom data type

When you select **Custom** in the **Data Type** field, you can define the meaning of each field in a multiple field log.

For example, a log (100300.351) contains three fields (100, 300.35, 1). The custom subtype allows you to specify what each of these fields is (integer, decimal, Boolean). For example:

- Initial log — 100300.351
- 3 Subtypes — Integer|decimal|boolean
- Custom Subtype — 100|300.35|1



The subtypes can include a maximum of 8 bytes (64 bits) of data. **Space Usage** displays the number of bytes and bits used. When the maximum is exceeded, this field states, in red, that the space has been exceeded, for example: Space Usage: 9 of 8 bytes, 72 of 64 bits.

Name/value custom type

If you select the **Name/Value Group** data type, you can add a custom type that includes a group of name/value pairs that you specify. You can then filter views and queries by these pairs, and use them in field match alarms.

These are some of the characteristics of this feature:

- The name/value group fields must be filtered using a regular expression.
- The pairs can be correlated so they are selectable in the **Correlation rule editor**.
- The values part of the pair can only be collected through the Advanced Syslog Parser (ASP).
- The maximum size for this custom type is 512 characters, which include the names. If it is larger than that, the values are cut off when collected. McAfee recommends that you limit the size and number of names.
- The names must consist of more than two characters.
- The name/value custom type can have up to 50 names.
- Each name in the name/value group is displayed in the global filter as <name of the group> - <name>.

Regular expression format for non-indexed custom types

Follow this formatting for non-indexed and indexed string, random string, and hashed string custom types:

- You can use `contains(<regular expression>)` syntax or just type a value into the non-indexed random string or hashed string fields, then filter custom types.
- You can use `regex()` syntax.
- With `contains()`, if you put a comma-separated filter into a non-indexed custom type field (Tom,John,Steve), the system performs a regular expression. The comma and asterisk act as a bar (|) and a period followed by the asterisk (.*). In a contains or non-indexed random string or hashed string field. If you type a character such as an asterisk (*), it is replaced with a period followed by the asterisk (.*).
- An invalid regular expression or a missing closing or opening parenthesis can cause an error telling you that you have a bad regular expression.
- You can only use a single `regex()` or `contains()` in non-indexed and indexed string, random string, and hashed string custom type filter fields.
- The Signature ID field now accepts `contains(<on part or all of a rule message>)` and `regex(<on part of a rule message>)`.
- A common search filter for `contains` is a single value, not a single value with a . * before and after.

Here are some common search filters:

- A single value
- Multiple values separated by commas, which are converted into a regular expression

- A `contains` statement with a `*` that acts like `.*`
- Advanced regular expressions, where you can use the `regex()` syntax

See *Description of `contains` and `regex` filters*.

See also

[Name/value custom types on page 320](#)

[Create custom types on page 319](#)

[Add Time custom types on page 320](#)

[Add name/value group custom type on page 321](#)

[Predefined custom types table on page 320](#)


Create custom types

Add custom types to use as filters if you have administrator rights.

Task

- 1 With the ESM selected on the system navigation tree, select **System Properties**, then click **Custom Types**.
- 2 Click **Add**, then complete the requested information.

Table 8-30 Option definitions

Option	Definition
Name	Type a name for this custom type.
Data Type	Select a data type from the drop-down list.
Events Field or Flows Field	Select which of the custom slots available for each event or flow is going to be occupied by this custom type.
Index Data	To filter by this custom type, select Index Data , which adds the custom type to the list of filters available for views, reports, and rules. The custom type doesn't appear in distribution components and isn't available in data enrichment, watch lists, or alarms. If you don't select this option, this type can be filtered only by regular expression.
Description	Type a description of this custom type.
Specify the number of subtypes	<p>If you select Long Custom or Short Custom in the Data Type field, you can add custom subtypes.</p> <ul style="list-style-type: none"> • Number of Subtypes — Select the number of subtypes that you want to add to the table. • Name column — Click each subtype, then type a name. • Data Type column — Click each subtype, then select the type of data for each subtype. <div>  If you select Boolean, validation ensures that they appear in groups of 8 subtypes. </div> <ul style="list-style-type: none"> • Length column — If you selected Integer or Unsigned Integer in the Data Type column, select the length of the data in bytes. An integer's length must be 1, 2, 4, or 8. • Manage Indexing — If you selected Accumulator Value in the Data Type field, click to enable indexes for each accumulator field.
Name list	If you select the Name/Value Group data type, add names for the name value pairs to this list. Type the name in the text field, and then click Add .

- 3 Click **OK**.

See also[Custom type filters on page 317](#)[Name/value custom types on page 320](#)[Add Time custom types on page 320](#)[Add name/value group custom type on page 321](#)[Predefined custom types table on page 320](#)

Predefined custom types table

If you have administrator privileges, you can view a list of the predefined custom types on the custom types table (**System Properties** | **Custom Types**).

If you do not have administrator privileges, refer to the list of predefined custom types in the [Intel Knowledge Center](#).

See also[Custom type filters on page 317](#)[Name/value custom types on page 320](#)[Create custom types on page 319](#)[Add Time custom types on page 320](#)[Add name/value group custom type on page 321](#)

Add Time custom types

You can add custom types that enable you to store time data.


Time - Seconds Precision stores time data down to the second. **Time - Nanosecond Precision** stores time down to the nanosecond. It includes a floating point number with nine precision values representing the nanoseconds.



If you select **Index** when adding this custom type, the field shows up as a filter on queries, views, and filters. It doesn't appear in distribution components and isn't available in data enrichment, watchlists, or alarms.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the system navigation tree, select the system, click the **Properties** icon , then click **Custom Types** | **Add**.
- 2 In the **Data Type** field, click **Time - Seconds Precision** or **Time - Nanosecond Precision**, fill in the remaining information, then click **OK**.

See also[Custom type filters on page 317](#)[Name/value custom types on page 320](#)[Create custom types on page 319](#)[Add name/value group custom type on page 321](#)[Predefined custom types table on page 320](#)

Name/value custom types

The name/value custom type consists of a group of name/value pairs that you specify. You can filter views and queries by these pairs, and use them in **Internal Event Match** alarms.

Here are some of the characteristics of this feature:

- The name/value group fields must be filtered using a regular expression.
- They can be correlated so they are selectable in the **Correlation rule editor**.

- The values part of the pair can only be collected through ASP.
- The maximum size for this custom type is 512 characters, which includes the names. Characters beyond 512 are cut off when collected. McAfee recommends that you limit the size and number of names.
- The names must consist of more than two characters.
- The name/value custom type can have up to 50 names.
- Each name in the name/value group is displayed in the global filter as <name of the group> - <name>.

See also

[Custom type filters on page 317](#)

[Create custom types on page 319](#)

[Add Time custom types on page 320](#)

[Add name/value group custom type on page 321](#)


[Predefined custom types table on page 320](#)

Add name/value group custom type

If you add a group of name/value pairs, you can filter views and queries by them and use them in **Internal Event Match** alarms.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select the system, then click the **Properties** icon .
- 2 Click **Custom Types**, then click **Add**.
- 3 In the **Data Type** field, click **Name/Value Group**, fill in the remaining information, then click **OK**.

See also

[Custom type filters on page 317](#)

[Name/value custom types on page 320](#)

[Create custom types on page 319](#)


[Add Time custom types on page 320](#)

[Predefined custom types table on page 320](#)

Add UCF and Windows event ID filters

One of the challenges for regulation compliance support is the ever-changing nature of regulations. Unified Compliance Framework (UCF) is an organization that maps the specifics of each regulation to harmonized control IDs. As regulations change, these IDs are updated and pushed to the ESM.

- You can filter by Compliance ID to select the required compliance or specific sub-components, or by Windows event IDs.

To...	Do this...
Add UCF filters	<ol style="list-style-type: none"> 1 In the Filters pane, click the filter icon next to the Compliance ID field. 2 Select the compliance values you want to use as filters, then click OK Run Query .
Add Windows event ID filters	<ol style="list-style-type: none"> 1 Click the filter icon next to the Signature ID. 2 On Filter Variables, select the Windows tab. 3 Type the Windows Event IDs (comma separated) in the text field, or select the values you want to filter by on the list.

See also[Filtering views on page 298](#)[Filter a view on page 298](#)[Select normalized IDs on page 299](#)

McAfee® Active Response searches

McAfee Active Response offers continuous visibility and insights into your endpoints, so you can identify breaches as they happen. It helps security practitioners query the current security posture, improve threat detection, and perform detailed analysis and forensic investigations

If Active Response is installed as an extension on a McAfee ePO device you have added to the ESM, you can run a search on Active Response from the ESM. The search generates a list of current endpoint data, allowing you to do the following:

- View the list of search results
- Create a watchlist populated with search results
- Append Active Response search data to an existing watchlist
- Add a data enrichment source populated with search results
- Export the search data

Searches are sent over DXL so it must be enabled on the **Connect** page of McAfee ePO properties (see *Run an Active Response search*).

Keep the following in mind when using Active Response on the ESM:

- DXL is not supported on HA Receivers.
- Dates from a search are in the format `2015-11-05T23:10:14.263Z` and are not converted to the ESM's date format.
- When you append data to a watchlist, the data isn't validated, which means you could add data to a watchlist that doesn't match its type.

See also[Run an Active Response search on page 323](#)[Manage Active Response search results on page 323](#)[Add an Active Response watchlist on page 325](#)

Run an Active Response search


You can run a search of Active Response from the ESM. The search generates a list of current endpoint data that meets the search criteria.

Before you begin

Add a McAfee ePO device with Active Response to the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Ensure that the McAfee ePO device is set up for the search.
 - a On the ESM console, click **McAfee ePO Properties**, then click **Connection**.
 - b Verify that **Enable DXL** is selected, and that an **Agent Wake-up Port** is specified (default is 8081).
- 2 On the ESM console, select a view with a **Table** component, such as **Event Analysis**.
- 3 Click an event, then click the **Menu** icon  on the component.

- 4 Select **Actions** | **Execute Active Response Search**, then select a predefined search type.

Option	Description
Full file information from a name, MD5, or SHA-1	Lists the file details of the source and destination IP address such as OS and name.
User detail search	Lists the details about the user.
Process information from source IP address and time	Lists source IP address process details for what established the connection.
Process information from destination IP address and time	Lists destination IP address process details for what established the connection.
CurrentFlow for IP address	Lists anyone connected to the same source or destination IP address.



Search types are grayed out if the table doesn't have the appropriate fields for the search.

The data is retrieved and listed on the **Active Response Details** page.

See also

[McAfee® Active Response searches on page 322](#)

[Manage Active Response search results on page 323](#)

[Add an Active Response watchlist on page 325](#)

Manage Active Response search results


After running an Active Response search, there are actions you can take to manage the data that was generated.

Before you begin

You must be viewing the results of an Active Response search (see *Run an Active Response search*).

Task

For details about product features, usage, and best practices, click **?** or **Help**.

1 On the Active Response **Details** page (see *Run an Active Response search*), select a row in the table, then click the **Menu** icon .

2 Select one of the options.

- **Create new watchlist from** - Creates a watchlist from the column you select on the drop-down list.



You can select more than one row on the table.


- **Append to watchlist from** - Appends the values from the column you select to an existing watchlist.



You can select more than one row on the table. Validation is not performed on the data selected from this table.

- **Export** - Export the current table to a CSV file.
- **Active Response search** - Perform another Active Response search on the data in the row you selected. If results are returned, the new results replace the current data set.

Table 8-31 Option definitions

Option	Action	Definition
Table		Lists the results of the Active Response search (see <i>Run an Active Response search</i>).
Menu icon	Create new watchlist from	Creates a new static watchlist of the values from the column that you select (see <i>Manage Active Response search results</i>). You can select multiple rows.
	Append to watchlist from	Appends the values from the column that you select to the existing watchlist that you select (see <i>Manage Active Response search results</i>). You can select multiple rows.  No validation is performed on the data selected from this table.
	Export	Exports the data to a .csv file.
	Active Response Search	Performs another Active Response search on the row that you select on the table. If there are results, the new data replaces the current data.

See also

[McAfee® Active Response searches on page 322](#)

[Run an Active Response search on page 323](#)

[Manage Active Response search results on page 323](#)

[Add an Active Response watchlist on page 325](#)

Add an Active Response data enrichment source


If Active Response is installed on a McAfee ePO device you have added to the ESM, you can add a data enrichment source populated with Active Response search results.

Before you begin

Add a McAfee ePO device with an Active Response extension to the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click the system, then click the **Properties** icon .
- 2 Click **Data Enrichment**, then click **Add**.
- 3 Complete the requested information on the **Main** tab.
- 4 On the **Source** tab, select Active Response in the **Type** field, then fill in the requested information.
- 5 Complete the information on the remaining tabs, then click **Finish**.

The source is added and the data you specified is enriched with the Active Response data.



The Active Response type is not listed if the ESM fails to pull the Active Response collectors over DXL.

Add an Active Response watchlist


If Active Response is installed on a McAfee ePO device you have added to the ESM, you can set up a dynamic watchlist populated with Active Response search results.

Before you begin

Add a McAfee ePO device with an Active Response extension to the ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click the system, then click the **Properties** icon .
- 2 Click **Watchlists**, then click **Add**.
- 3 Complete the **Main** tab, selecting **Dynamic**.
- 4 On the **Source** tab, select Active Response in the **Type** field, then fill in the requested information.
- 5 Complete the information on the remaining tabs, then click **Finish**.

The watchlist is added and collects the data you specified from Active Response searches.



The Active Response type is not listed if the ESM fails to pull the Active Response collectors over DXL.

See also

[McAfee® Active Response searches on page 322](#)

[Run an Active Response search on page 323](#)

[Manage Active Response search results on page 323](#)

9

Managing cases

Use the ESM case manager to assign and track work items and support tickets associated with network events. To access this feature, you must be part of a group that has the **Case Management User** privilege enabled.

There are five ways to add a case:

- On the **Case Management** view
- On the **Cases** pane, without linking to an event
- On the **Event Analysis** view, linking it to an event
- When you set up an alarm
- On a triggered alarm notification

Contents


- *Add a case*
- *Create a case from an event*
- *Add events to an existing case*
- *Edit or close a case*
- *View case details*
- *Add case status levels*
- *Email cases*
- *View all cases*
- *Generate case management reports*

Add a case

Your first step in tracking a task generated as the result of a network event is to add a case to the case management system.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the **Cases** pane, click the **Add Case** icon .
- 2 Fill in the information requested, then click **OK**.

The case is added to the **Cases** pane of the user the case is assigned to. If you selected **Email case**, an email is also sent (see *Email a case*).

See also

[Create a case from an event on page 328](#)

[Add events to an existing case on page 328](#)

[Edit or close a case on page 330](#)

[View case details on page 331](#)

[Add case status levels on page 332](#)

[Email cases on page 333](#)

[View all cases on page 333](#)


[Generate case management reports on page 334](#)

Create a case from an event

To track an event on the **Event Analysis** view, create a case. This enables workflow tracking.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the views list, select **Event Views | Event Analysis**.
- 2 Click the event, click the menu icon , then click **Actions | Create a new case**.
- 3 Complete the information requested, then click **OK** to save the case.

The new case includes the event data in the **Message** table.

See also

[Add a case on page 327](#)

[Add events to an existing case on page 328](#)

[Edit or close a case on page 330](#)

[View case details on page 331](#)

[Add case status levels on page 332](#)

[Email cases on page 333](#)

[View all cases on page 333](#)



[Generate case management reports on page 334](#)

Add events to an existing case

To keep track of actions taken in response to events, add one or more events to an existing case.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the views pane, select **Event Views** from the list of views, then click **Event Analysis**.
- 2 Select the events, then do one of the following:
 - Click the **Assign Events to a Case or Remedy** icon  and select **Add events to a case**.
 - Click the **Menu** icon , highlight **Actions**, then click **Add events to a case**.
- 3 Select the case and click **Add**.

The **Case Details** page lists the event ID in the **Messages** table.

- 4 Click **OK**, then click **Close**.

Table 9-1 Option definitions

Option	Definition
Summary	A brief descriptive summary of the case. It appears in the Cases pane. Type a maximum of 255 characters.
Case ID	A unique, system-generated number given to the case once it has been added. This number can't be changed.
Assignee	The users or groups that case is assigned to. Lists all the users and user groups who have case management rights (see <i>Set up user groups</i>). Select the user or group on the list.
take	Click to reassign the case to yourself.
Severity	The severity of the case. 1 through 20 = Green 21 through 40 = Blue 41 through 60 = Yellow 61 through 80 = Brown 81 through 100 = Red Select the severity level for this case.
Organization	(Optional) The organization the case is assigned to. You can add an organization by clicking Organization , then clicking Add .
Status	The status of the case. The case manager comes with two statuses: Open (default) and Closed . To add more statuses that cases can be assigned to, click Status , then click Add and enter the information requested.
Created	The date the case was created.
Last Updated	The last time the case was changed.
Notes	Records actions taken and changes made to a case and any notes that you add. The following actions and changes will be recorded in this section automatically after you add the case: <ul style="list-style-type: none"> • Case opened • Case closed • Changes to the summary • Case is reassigned • Severity is changed • Organization is changed • Events are changed <p>The note includes the type of action taken or change made, the date and time, and the name of the user. In the case of a change, it also shows the old value and the new value, for example:</p> <pre>---- Severity Changed on 04-22-2009 at 09:39 old: Low new: High</pre>
History	Lists the users who have accessed the case.
Message table	Lists the events that are associated with the case. To view the details of an event, click the event on the table, then click Show Details .
E-mail Case	Allows you to email the case to the address you specify.

See also
[Add a case on page 327](#)
[Create a case from an event on page 328](#)
[Edit or close a case on page 330](#)
[View case details on page 331](#)
[Add case status levels on page 332](#)
[Email cases on page 333](#)
[View all cases on page 333](#)
[Generate case management reports on page 334](#)




Edit or close a case

If you have **Case Management Administrator** privileges, you can modify any case on the system. If you have **Case Management User** privileges, you can modify only cases that are assigned to you.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 Access **Case Details** in one of these ways.

For...	Do this...
A case assigned to you	<ol style="list-style-type: none"> 1 Select the case on the Cases pane. 2 Click the Edit Case icon .
A case not assigned to you	<ol style="list-style-type: none"> 1 Click the Open Case Management icon  in the Cases pane. 2 Select the case to be modified. 3 Click the Edit Case icon  at the bottom of the view.

- 2 Edit the settings or close the case in the **Status** field.

- 3 Click **OK** to save the changes.

The changes are recorded in the **Notes** section of the **Case Details** page. If you closed the case, it no longer appears on the **Cases** pane, but remains on the **Case Management** list with the status changed to **Closed**.

See also
[Add a case on page 327](#)
[Create a case from an event on page 328](#)
[Add events to an existing case on page 328](#)
[View case details on page 331](#)
[Add case status levels on page 332](#)
[Email cases on page 333](#)
[View all cases on page 333](#)
[Generate case management reports on page 334](#)

View case details

Take action on any case.

Before you begin

Verify that you have administrator rights or belong to an access group with case management permission.

Task


- 1 On the dashboard, click  and select **Investigation Panel**.
A summary of open cases appears on the left side of the dashboard.
- 2 Use the drop-down arrow to expand the case you want to view and click **View Case Management**.
The **Case Management** view opens, listing all cases on the system.
- 3 Review the data on the **Notes** and **Source Events** tabs.
- 4 For further details, double-click the case, then review the information about the **Case Details** page.

Table 9-2 Option definitions

Option	Definition
Summary	A brief descriptive summary of the case. It appears in the Cases pane. Type a maximum of 255 characters.
Case ID	A unique, system-generated number given to the case once it has been added. This number can't be changed.
Assignee	The users or groups that case is assigned to. Lists all the users and user groups who have case management rights (see <i>Set up user groups</i>). Select the user or group on the list.
take	Click to reassign the case to yourself.
Severity	The severity of the case. 1 through 20 = Green 21 through 40 = Blue 41 through 60 = Yellow 61 through 80 = Brown 81 through 100 = Red Select the severity level for this case.
Organization	(Optional) The organization the case is assigned to. You can add an organization by clicking Organization , then clicking Add .
Status	The status of the case. The case manager comes with two statuses: Open (default) and Closed . To add more statuses that cases can be assigned to, click Status , then click Add and enter the information requested.
Created	The date the case was created.
Last Updated	The last time the case was changed.

Table 9-2 Option definitions *(continued)*

Option	Definition
Notes	<p>Records actions taken and changes made to a case and any notes that you add. The following actions and changes will be recorded in this section automatically after you add the case:</p> <ul style="list-style-type: none"> • Case opened • Case closed • Changes to the summary • Case is reassigned • Severity is changed • Organization is changed • Events are changed <p>The note includes the type of action taken or change made, the date and time, and the name of the user. In the case of a change, it also shows the old value and the new value, for example:</p> <pre>---- Severity Changed on 04-22-2009 at 09:39 old: Low new: High</pre>
History	Lists the users who have accessed the case.
Message table	Lists the events that are associated with the case. To view the details of an event, click the event on the table, then click Show Details .
E-mail Case	Allows you to email the case to the address you specify.



See also[Add a case on page 327](#)[Create a case from an event on page 328](#)[Add events to an existing case on page 328](#)[Edit or close a case on page 330](#)[Add case status levels on page 332](#)[Email cases on page 333](#)[View all cases on page 333](#)[Generate case management reports on page 334](#)

Add case status levels

The case manager comes with two status levels: **Open** and **Closed**. You can add other statuses that cases can be assigned to.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the **Cases** pane, click the **Open Case Management** icon .
- 2 On the **Case Management** view, click the **Case Management Settings** icon  on the bottom toolbar, then click **Add**.
- 3 Type a name for the status, then select if you want this status to be the default for new cases.
- 4 Select if you want cases with this status to be shown in the **Cases** pane, then click **OK**.

See also[Add a case on page 327](#)[Create a case from an event on page 328](#)[Add events to an existing case on page 328](#)[Edit or close a case on page 330](#)[View case details on page 331](#)[Generate case management reports on page 334](#)





Email cases

Set the system to automatically send an email message to the person or group a case is assigned to, every time a case is added or reassigned.

Before you begin

You must have **Case Management Administrator** privileges.

You can also email a case notification manually, and include case notes and event details.

To...	Do this...
Email a case automatically	<ol style="list-style-type: none">1 On the Cases pane, click the Open Case Management icon .2 Click the Case Management Settings icon .3 Select Send an email when a case is assigned, then click Close. <div> Email addresses for the users must be on the ESM (see <i>Setup users</i>).</div>
Email an existing case manually	<ol style="list-style-type: none">1 On the Cases pane, select the case you want to email, then click the Edit Case icon .2 On Case Details, click Email Case, then fill in the From and To fields.3 Select whether you want to include the notes and attach a CSV file of the event details.4 Type any notes you want to include in the email message, then click Send.

See also[Add a case on page 327](#)[Create a case from an event on page 328](#)[Add events to an existing case on page 328](#)[Edit or close a case on page 330](#)[View case details on page 331](#)[Generate case management reports on page 334](#)


View all cases








Manage all cases on the system, whether they are currently open or closed.

Before you begin

Verify that you have administrator rights or belong to an access group with case management permission.

Task

- 1 On the dashboard, click  and select **Investigation Panel**.
A summary of open cases appears on the left side of the dashboard.
- 2 Use the drop-down arrow to expand the case you want to view and click **View Case Management**.
The **Case Management** view opens, listing all cases on the system.
- 3 Do any of the following:

To do this...	Do this...
Add a case	Click the Add Case icon  on the toolbar at the bottom of the view.
View or edit the selected case	Click the Edit Case icon  on the toolbar at the bottom of the view.
Email the selected case	Click the Email Case icon  on the toolbar at the bottom of the view.
Set a case up to send an email when a case is added or changed	Click the Case Management Settings icon  on the toolbar at the bottom of the view.
Add or edit the statuses available for cases	Click the Case Management Settings icon  and click Add , Edit , or Delete .
View the notes, history, and source events for the case you select	Click Notes , History , or Source Events . When you click Source Events , the Source Event details tabs open. If the tabs aren't visible or if they are visible and you want to hide them, click the View Source Event details icon  on the toolbar at the bottom of the view. The History tab records any time a user views a case. If the same user views a case more than once in five minutes, it doesn't update the record each time.
Change Source Events columns	Click the Source Events tab, then click Edit visible columns in Source Events tab .
Filter the cases	On the Filters pane, select or type the data you want to filter the cases by, then click the Run Query icon  . The list of cases changes to show only the ones that meet the filter criteria.

See also

[Add a case on page 327](#)
[Create a case from an event on page 328](#)
[Add events to an existing case on page 328](#)
[Edit or close a case on page 330](#)
[View case details on page 331](#)
[Generate case management reports on page 334](#)

Generate case management reports

There are six case management reports available on the ESM.

Task

For details about product features, usage, and best practices, click ? or Help.

- 1 On the **System Properties** page, click **Reports | Add**.
- 2 Complete sections 1, 2, and 3.
- 3 In section 4, select **Query CSV**.
- 4 In section 5, select the case management report to run.
 - **Case Management Summary** — Includes case ID numbers, the severity assigned to the cases, their status, the users they are assigned to, the organizations where they are assigned (if any), the date and time that the cases were added, the date and time that the cases were updated (if they have been), and the case summaries.
 - **Case Management Details** — Includes all information in the **Case Management Summary** report as well as the ID numbers of the events linked to the cases and the information included in the notes sections of the cases.
 - **Case Time to Resolution** — Shows the length of time that it took between status changes (for example, the differential between the **Open** time stamp and **Closed** time stamp). By default, it lists the cases with a status of **Closed** by **Case ID** number as well as severity, organization, **Created** date, last update, summary, and time difference.
 - **Cases per Assignee** — Includes the number of cases assigned to a user or group.
 - **Cases per Organization** — Includes the number of cases per organization.
 - **Cases per Status** — Includes the number of cases per status type.
- 5 Complete section 6 (see *Description of contain and regex filters*), then click **Save**.

The report is saved and added to the **Reports** list.

See also

[Add a case on page 327](#)
[Create a case from an event on page 328](#)
[Add events to an existing case on page 328](#)
[Edit or close a case on page 330](#)
[View case details on page 331](#)
[Add case status levels on page 332](#)
[Email cases on page 333](#)
[View all cases on page 333](#)

10 Working with the Asset Manager

The **Asset Manager** provides a centralized location that allows you to discover, manually create, and import assets.

Contents

- ▶ *How Asset Manager works*
- ▶ *Asset Sources*
- ▶ *Manage vulnerability assessment sources*
- ▶ *Zone Management*
- ▶ *Asset, threat, and risk assessment*
- ▶ *Manage known threats*
- ▶ *Select data to view in Scorecard*

How Asset Manager works

Asset Manager provides a centralized location that allows you to discover, manually create, and import assets. Asset Manager presents a list of the assets on your network. An asset is any device with an IP address that has been added to ESM. Several tabs on the Asset Manager page help you manage assets and related items.

You can create a group to contain one or more assets. You can perform the following operations on the entire group:

- Change the attributes for all assets in a group.



This change is not persistent. If you add an asset to a changed group, the asset doesn't inherit the previous settings automatically.

- Use drag-and-drop operations.
- Rename groups.

Asset groups allow you to categorize assets in ways that are unavailable with asset tagging. For example, if you want to create an asset group for each building on your campus. The asset consists of an IP address and a collection of tags. The tags describe the operating system the asset is running and a collection of services for which the asset is responsible.

Asset tags are defined in one of two ways:

- When the system retrieves an asset.
- When the user adds or edits an asset.

If the system sets up the tags, they are updated each time the asset is retrieved if they have changed. If the user sets up the tags, the system does not update the tag when the asset is retrieved, even if they have changed. If you add or edit the tags of an asset but you want the system to update them when the asset is retrieved, click **Reset**. You must complete this action each time you change the tag settings.

Configuration management is part of standard compliance regulations such as PCI, HIPPA, and SOX. It allows you to monitor any changes that might be made to the configuration of your routers and switches, thus preventing system vulnerabilities. On the ESM, the configuration management feature enables you to:

- Set the frequency with which devices must be polled.
- Select the discovered devices on which to check configuration.
- Identify a retrieved configuration file as the default for the device.
- View the configuration data, download the data to a file, and compare the configuration information of the two devices.

Contents

- [Manage assets](#)
- [Define old assets](#)

Manage assets

An asset is any device on the network that has an IP address. You can create assets, change their tags, create asset groups, add asset sources, and assign an asset to an asset group. You can also manipulate the assets learned from vulnerability assessment vendors.

Before you begin

Verify that you have administrator rights or belong to an access group with device management permission.

Task



- 1 From the dashboard, click  and select **Asset Manager**.
- 2 Select the **Asset** tab.
A list of assets is displayed.
- 3 To sort the list, click the column headings.
- 4 To view the details for an asset, select the asset and then click the assets icon .
- 5 To assign an asset to a group, drag and drop it from the Assets pane to an asset group.
- 6 Configure the assets.

Table 10-1 Main menu options

Option	Definition
New Group	Add an asset group. Type a name for the group and select its criticality.
New Asset	Add an asset.
New Asset Filter Group	Add an asset filter group. This option is only accessible if this is the first item being added to the asset tree or if you highlight an existing group.

Table 10-1 Main menu options *(continued)*

Option	Definition
File Import from file	Import a .csv file to the location you have selected on the list of assets. Format the asset data in the .csv file like this: <pre>Hostname, IPAddress, Mask, ZoneName, UsrSeverity, UseCalcSeverity, TagCount, TagGroupName:TagName</pre> Add one <code>TagGroupName:TagName</code> for each tag you have (<code>TagCount</code>). Each asset must be on its own line.
File Export to file	Export the selected asset files.
Edit Modify	Change the selected asset or asset group.
Edit Use in risk calculation or Ignore in risk calculation	Sets whether to use the asset when calculating the overall risk for your enterprise. Use in risk calculation is the default setting.
Edit Delete	Delete the selected group or asset. If you select a group, you are asked if you want to delete the group and its assets or just the group. If you select only the group, the assets are reassigned to the Unassigned folder.
Tools Create DEM Database Server	Add an asset as a database server to a DEM device on the system.
Tools Create Receiver Data Source	Add an asset as a data source to a Receiver on the system.
Tagging	To define its attributes and act as filters, add tags to the selected asset.

Table 10-2 Create a new asset






Option	Definition
IP Address	The IP address for this asset.
MAC Address	(Optional) Type the MAC address for this asset.
GUID	(Optional) The globally unique identifier for this asset.
Operating System	(Optional) This asset's operating system.
Zone	The zone this asset is in. <div>  <p>If a zone is assigned to an asset or group of assets, users that do not have permission to that zone do not have access to those assets.</p> </div>
Criticality	How critical this asset is to your enterprise: 1 = lowest criticality, 100 = highest criticality. Criticality and severity of a threat are used to calculate the overall event severity to your enterprise.
Tags table	Tags for this asset.
New Category Tag 	Adds a new category to the list of tags. Type a name for the category and select if you want this category to be used in event severity calculation.
New Tag 	Adds a new tag. Type a name for the tag and select if you want this tag to be used in event severity calculation.
Edit Tag 	Opens the selected tag for editing.
Remove Tag 	Deletes the selected tag.

Table 10-3 New asset advanced settings






Option	Definition
Use this Asset's criticality	Always use the assigned asset criticality when computing event severity.
Use Overall Calculated criticality	Always use the greatest criticality value when computing event severity. <div>  If you select this option and you changed the rate in the Criticality field, the Calculate and Groups buttons are active. </div>
Calculate	Calculates the overall severity, which is added to the Calculate field.
Groups	View a list of the groups this asset belongs to and the criticality for each group.
Reset	Have the system automatically set the tags for this asset.

Table 10-4 Create a new asset filter group

Option	Definition
Name	The name for the filter asset group.
IP Address/Mask	The IP address or address/mask for this group.
Zone	Assigns the group to a zone. If the zone you need is not listed, click Zone and add it.
Criticality	The criticality level for this group. This setting represents how critical the asset is to your operation.
Tags list	The tags that are applied as filters to this group. You can define a filter group based on the existence of one or more asset tags. The tags that are set do not define the exclusive set of tags an asset must have. The asset can have other tags and still be a member of the filter group.
New Category Tag 	Adds a category to the list of tags. Type a name for the category and select if you want this category to be used in event severity calculation.
New Tag 	Add a tag. Type a name for the tag and select if you want this tag to be used in event severity calculation.
Edit Tag 	Allows you to edit the selected tag.
Remove Tag 	Deletes the selected tag.

See also

[Manage asset sources on page 341](#)

[Manage vulnerability assessment sources on page 343](#)

[Manage known threats on page 348](#)


[Define old assets on page 340](#)

Define old assets

The **Old Assets** group on the **Asset Manager** allows you to store assets that haven't been detected in the time that you define.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Click the **Asset Manager** quick launch icon .
- 2 On the **Asset** tab, double-click the **Old Assets** group from the list of assets.
- 3 Select the number of days since an asset was last detected before it must be moved to the **Old Assets** folder, then click **OK**.

See also

[Manage assets on page 338](#)

Asset Sources

You can retrieve data from your **Active Directory**, if you have one, or an Altiris server using **Asset Sources**.

Active Directory allows you to filter event data by selecting the retrieved users or groups in the **Source User** or **Destination User** view query filter fields. This improves your ability to provide compliance data for requirements like PCI. Altiris and **Active Directory** retrieve assets such as computers with IP addresses, and add them to the assets table.



In order to retrieve assets on Altiris, you must have **Asset Manager** privileges on the Altiris Management Console.

Active Directory doesn't typically store IP address information. The system uses DNS to query for the address once it gets the name from **Active Directory**. If it can't find the address of the computer, it doesn't get added to the **Assets** table. For this reason, the DNS server on the system needs to contain the DNS information for **Active Directory** computers.

You can add IP addresses to **Active Directory**. If you do this, modify the `networkAddress` attribute on your computer objects so the system uses those IP addresses instead of querying DNS.

See also

[Manage asset sources on page 341](#)

Manage asset sources

Retrieve data from your Active Directory or an Altiris server.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 Click the **Asset Manager** quick launch icon , then click the **Asset Sources** tab.

The **Asset Sources** tree shows the ESM and Receivers on the system, and their current asset sources.



An ESM can have one and Receivers can have multiple asset sources.

- 2 Select a device then select either of the available actions.

Table 10-5 Option definitions

Option	Definition
Table	View the ESM and Receivers on the system, and their current asset sources.
Add	Add a new asset source to the ESM or one of the Receivers.
Edit	Change the selected asset source.
Remove	Delete the selected asset source.
Retrieve	Retrieve the data now.
Write	Click when you change any asset source settings, to write the changes to the devices.

Table 10-6 Option definitions

Option	Definition
Enabled	Select if you want to enable automatic retrieval. If you don't select it, you can still retrieve data manually by clicking Retrieve on the Asset Sources page. If it is selected, the data will be retrieved at the time interval specified in the Retrieve Data field.
Type	Select if this is an active directory or Altiris asset source.
Name	Type a name for the asset source
Zone	To assign a data source to one, select a zone.
Priority	Select the priority you want this asset source to have if it discovers an asset at the same time as Vulnerability Assessment or Network Discovery .
IP Address	Type the IP address for this asset source.
Port	Select the port for this asset source.
Use TLS or Use SSL	Select if you want to use an encryption protocol for the data. Active directory uses TLS; Altiris uses SSL.
User Name	Type the user name required to access the asset source.
Password	Type the password required to access the asset source.
Search Base	For Active Directory, type the distinguished name of the object where you want the search for assets to begin (dc=mcafee,dc=com).
Proxy information	For Altiris, type the IP address, the port it is listening on, the name of the proxy user, and the password for the proxy server.
Retrieve Data	To retrieve the data automatically, select the frequency.
Connect	Click to test the connection to the Altiris server.

Table 10-7 Option definitions

Option	Definition
Device	Lists the devices the changes are being applied to.
Status	Shows the status of the process for each device.

See also[Manage assets on page 338](#)[Manage vulnerability assessment sources on page 343](#)[Manage known threats on page 348](#)[Asset Sources on page 341](#)

Manage vulnerability assessment sources

You can retrieve data from a variety of VA vendors using **Vulnerability Assessment**. To communicate with the desired VA sources, you must add the source to the system. Once a source is added to the system, you can retrieve the VA data.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 Click the **Asset Manager** quick launch icon , then click the **Vulnerability Assessment** tab.
- 2 Add, edit, remove, or retrieve VA sources, then write them to the device.
- 3 Click **OK**.

Table 10-8 Option definitions

Option	Definition
Device	Lists the devices that are being removed.
Status	Shows the status of the process for each device being removed.

See also

[Manage asset sources on page 341](#)

[Manage assets on page 338](#)

[Manage known threats on page 348](#)

Zone Management

Zones can be used to categorize devices and data sources on your network.

This enables you to organize devices and the events they generate into related groupings by geographic location and IP address. For example, if you have offices on the East Coast and the West Coast and you want the events generated by each office to be grouped together, you add two zones and assign the devices whose events must be grouped to each of the zones. To group the events from each office by specific IP addresses, you add subzones to each of the zones.

See also

[Manage zones on page 343](#)

[Add a zone on page 344](#)

[Export zone settings on page 345](#)

[Import zone settings on page 345](#)

[Add a subzone on page 347](#)

Manage zones

Zones help you categorize your devices and data sources by geolocation or ASN. You must add zones, either individually or importing a file exported from another machine, and assign the devices or data sources to the zones.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 Click the **Asset Manager** quick launch icon , then select **Zone Management**.
- 2 Add a zone or subzone, edit or remove existing zones, or import or export zone settings.
- 3 Rollout any changes you make, then click **OK**

Table 10-9 Option definitions

Option	Definition
Add Zone	Add a new zone to the ESM.
Add Sub-zone	Add a sub-zone to the selected zone to break it down by IP addresses.
Edit	Change the settings of the selected zone or sub-zone.
Remove	Delete the selected zone or sub-zone.
Import	Import a zone definition file or device to zone assignment file exported from another ESM.
Export	Export the zone settings on your ESM.
Rollout	Roll out any changes you have made to the ESM.

Table 10-10 Option definitions

Option	Definition
Select column	Select the devices you want to roll the changes out to.
Device column	View the devices on the system.
Status column	View the status of the rollout for each device.

See also

[Zone Management on page 343](#)

[Add a zone on page 344](#)

[Export zone settings on page 345](#)

[Import zone settings on page 345](#)

[Add a subzone on page 347](#)

Add a zone

The first step in zone management is to add the zones used to categorize your devices and data sources. They can be added individually using the **Add Zone** feature or you can import a file that was exported from another system. When a zone is added, you can edit its settings when required.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 Click the **Asset Manager** quick launch icon , then click **Zone Management**.
- 2 Enter the information requested and assign devices to the zone, then click **OK**.

Table 10-11 Option definitions

Option	Definition
Name	Type a name for this zone.
Use as the default zone assignment	Select if you want this zone assignment to be the default for events generated by the devices assigned to this zone that do not fall into one of its sub-zones.
Geolocation	To use geolocation to define the boundaries of this zone, click the Filter icon, then select the location you want included in this zone.
ASN	To define the boundaries of this zone using ASN, which uniquely identifies each network on the Internet, enter the numbers in this field.
Assigned Devices	Select the devices that you want to assign to this zone.

See also[Zone Management on page 343](#)[Manage zones on page 343](#)[Export zone settings on page 345](#)[Import zone settings on page 345](#)[Add a subzone on page 347](#)

Export zone settings

You can export the zone settings from your ESM so you can import them to another ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 Click the **Asset Manager** icon , then click **Zone Management**.
- 2 Click **Export**, then select the type of file you want to export.
- 3 Click **OK** and select the file to download now.

Table 10-12 Option definitions

Option	Definition
Export zone definition file	Export a file that includes the parent zones and their sub-zones, as well as all of the details regarding their settings.
Export device to zone assignment file	Export a file that includes the devices and the zone they are assigned to.

See also[Zone Management on page 343](#)[Manage zones on page 343](#)[Add a zone on page 344](#)[Import zone settings on page 345](#)[Add a subzone on page 347](#)

Import zone settings

This import feature allows you to import a zone file as is, or edit the data before importing it.

Before you begin

Export a file of zone settings from another ESM so that it can be imported to your ESM.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 Open the zone settings file that you want to import.
 - If this file is an import zone definition file, it has eight columns: Command, Zone Name, Parent Name, Geo Location, ASN, Default, IPStart, and IPStop.
 - If it is an import device to zone assignment file, it has three columns: Command, Device Name, and Zone Name.
- 2 Enter commands in the **Command** column to specify the action to be taken for each line when it is imported.
 - `add` — Import the data in the line as it is.
 - `edit` — (Zone definition file only) Import the data with any changes you make to the data.



To make changes to a subzone range, you must remove the existing range, then add the range with the changes. You can't edit it directly.



- `remove` — Delete the zone matching this line from the ESM.
- 3 Save the changes you made, then close the file.
 - 4 Click the **Asset Manager** quick launch icon , then click the **Zone Management** tab.
 - 5 Click **Import**, then select the type of import it will be.
 - 6 Click **OK**, then locate the file to be imported and click **Upload**.
The system notifies you if errors are detected in the file.
 - 7 If there are errors, make the necessary corrections to the file and try again.
 - 8 Roll out the changes to update the devices.

Table 10-13 Option definitions

Option	Definition
Import zone definition file	Import a file that includes the parent zones and their sub-zones, as well as all details regarding their settings. <div>  To make changes to a subzone range, you must remove the existing range, then add the range with the changes. You can't edit it directly. </div>
Import device to zone assignment file	Import a file that includes the devices and the zone they are assigned to.

See also

[Zone Management on page 343](#)

[Manage zones on page 343](#)

[Add a zone on page 344](#)

[Export zone settings on page 345](#)

[Add a subzone on page 347](#)

Add a subzone

Once you have added a zone, you can add subzones to further categorize the devices and events by IP address.

Before you begin

Add zones on the **Zones Management** tab.

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 Click the **Asset Manager** quick launch icon , then click the **Zone Management** tab.
- 2 Select a zone, then click **Add Sub-zone**.
- 3 Fill in the information requested, then click **OK**.

Table 10-14 Option definitions

Option	Definition
Name	Type a name for this sub-zone
Description	Type a description of this sub-zone
Ranges table	View the IP address ranges for this sub-zone.
Add	Add IP address ranges as well as geolocation or ASN information for this range.
Edit	Change the selected range.
Remove	Delete the selected range.

Table 10-15 Option definitions

Option	Definition
Start IP and End IP	Type the beginning and ending IP address for this range.
Geolocation	If you want this range to have a different geolocation than the default, select the override geolocation in this field.
ASN	If you want this range to have a different ASN than the default, type the override ASN in this field.

See also

[Zone Management on page 343](#)

[Manage zones on page 343](#)

[Add a zone on page 344](#)

[Export zone settings on page 345](#)

[Import zone settings on page 345](#)

Asset, threat, and risk assessment

McAfee Threat Intelligence Services (MTIS) and the vulnerability assessment sources on your system generate a list of known threats. The severity of these threats and the criticality of each of your assets are used to calculate the level of risk to your enterprise.

Asset Manager

When you add an asset to your **Asset Manager** (see *Manage assets*), you assign a criticality level. This setting represents how critical the asset is to your operation. For example, if you have one computer managing your enterprise setup and it doesn't have a backup, its criticality is high. If, however, you have two computers managing your setup, each with a backup, the criticality level is considerably lower.

You can select whether to use or ignore an asset in risk calculation for your enterprise on the **Edit** menu of the **Asset** tab.

Threat Management

The **Threat Management** tab on the **Asset Manager** shows a list of known threats, their severity, the vendor, and whether they are used when calculating risk. You can enable or disable specific threats so that they are or are not used to calculate risk. You can also view the details for the threats on the list. These details include recommendations for dealing with the threat as well as countermeasures you can use.

Pre-defined views

Three pre-defined views (see *Working with ESM views*) summarize and display asset, threat, and risk data:

- **Asset threat summary** — Displays the top assets by risk score and threat levels, and threat levels by risk.
- **Recent threat summary** — Displays recent threats by vendor, risk, asset, and available protection products.
- **Vulnerability summary** — Displays vulnerabilities by threats and assets.

Details of individual items on these views can be accessed from the component menus.

Custom views

Options have been added to the **Query Wizard** to enable you to set up custom views (see *Add a custom view*) that display the data you need.

- On the **Dial Control** and **Count** components, you can display the average enterprise risk score and the total enterprise risk score.
- On the **Pie Chart**, **Bar Chart**, and **List** components, you can display the assets at risk, product threat protection, threat by asset, threat by risk, and threat by vendor.
- On the **Table** component, you can display assets, most recent threats, top assets by risk score, and top threats by risk score.


Manage known threats

Select which known threats to use in risk calculations.

Each threat has a severity rating. This rating and the criticality rating for your assets are used to calculate the overall severity of a threat to your system.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM console, click the **Asset Manager** quick launch icon .
- 2 Click the **Threat Management** tab to display the list of known threats.
- 3 Select a known threat, then do one of the following:
 - Click **Threat Details** to view the details about the threat.
 - If the **Calculate Risk** column says **Yes** and you do not want it to be used in risk calculations, click **Disable**.
 - If the **Calculate Risk** column says **No**, and you want it to be used in risk calculations, click **Enable**.
- 4 Click **OK**.

See also

[Manage asset sources on page 341](#)

[Manage vulnerability assessment sources on page 343](#)

[Manage assets on page 338](#)

Select data to view in Scorecard

To view asset audit data in Scorecard, you must select the data that ESM pulls from McAfee ePO.

Before you begin

ePolicy Orchestrator must be running with Policy Auditor.

When selecting the data to show in scorecard, consider the volume of data involved and its effect on performance. Rules are granular and using them results in large amounts of data being displayed. Benchmarks are sets of rules and display one data point for multiple rules.

Task

- 1 Open **Asset Manager** and select the **Scorecard** tab.

All attached McAfee ePO devices are listed.
- 2 For each device, select the data to display - **none**, **benchmarks**, or **benchmarks and rules**.

See also

[How Scorecard view works on page 351](#)

11

Scorecard

See Policy Auditor audit results in the ESM Scorecard view.

The Scorecard requires McAfee ePO with Policy Auditor. Once this requirement is met, you can select the data to pull into Scorecard.

The two tables in the Scorecard view are bound to each other. By default, the Asset Groups table is bound to the Benchmarks table. You can change the binding so that the Benchmarks Groups table is bound to the Asset Groups table.

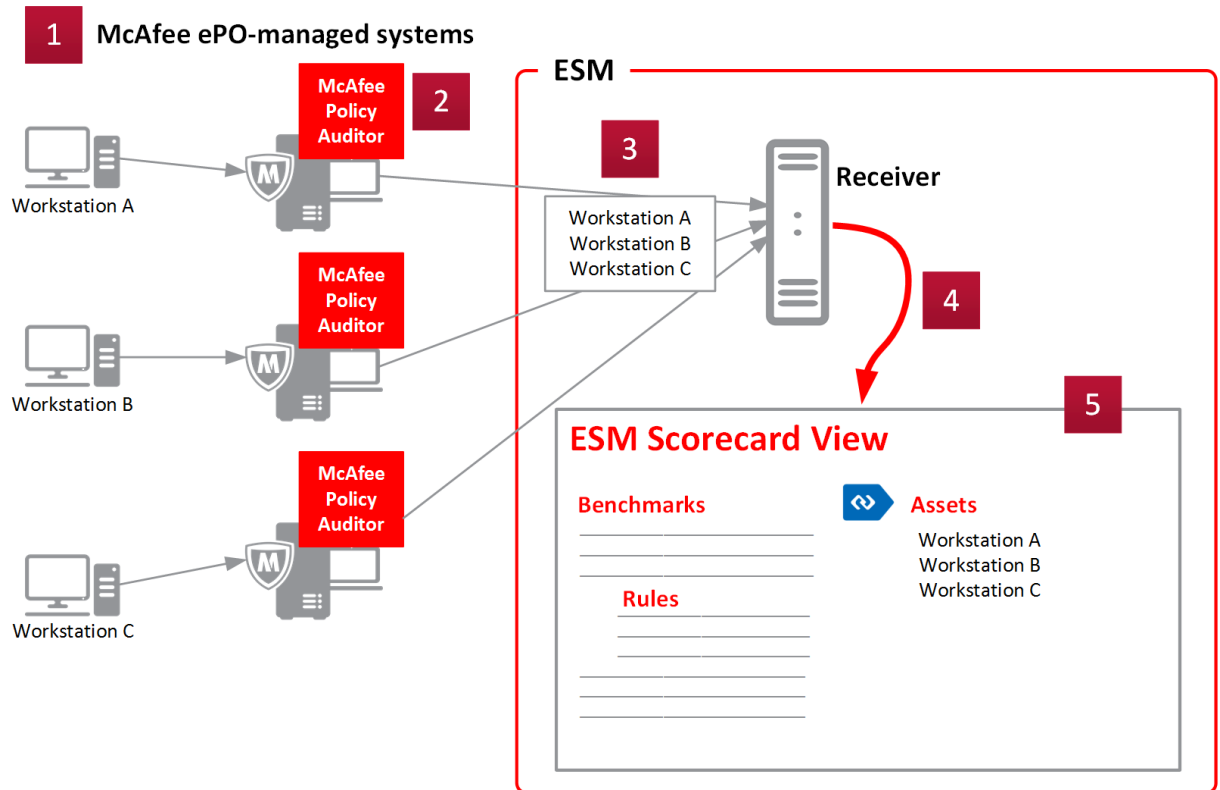
Contents

- ▶ *How Scorecard view works*
- ▶ *Select data to view in Scorecard*
- ▶ *View Policy Auditor data in Scorecard*
- ▶ *Configure Scorecard view*
- ▶ *Configure benchmark groups*

How Scorecard view works

Scorecard view presents Policy Auditor data in the ESM interface.

You can evaluate system vulnerability on the Scorecard tab of Asset Manager.



- 1 ePolicy Orchestrator is configured to audit system assets with Policy Auditor.
- 2 Policy Auditor feeds audit results to ePolicy Orchestrator.
- 3 ePolicy Orchestrator sends audit results to the Event Receiver.
- 4 The Event Receiver makes audit data available in ESM.
- 5 Scorecard view presents the audit data in a graphic interface. You can view data as text values or as percent bars.

Scorecard view shows the percentage of rules/benchmarks that an asset or group of assets has passed. You can also select an asset or group of assets and see which rules it passed.

Two statistics ribbons above the data tables show 1) statistics for the average benchmark score, 2) how many assets the score represents, and 3) the trend over the last 6 months. The trend line appears only if there are at least two data points, which is about two weeks of data.

See also

[Configure Scorecard view on page 354](#)
[View Policy Auditor data in Scorecard on page 353](#)
[Configure benchmark groups on page 354](#)
[Select data to view in Scorecard on page 349](#)

Select data to view in Scorecard

To view asset audit data in Scorecard, you must select the data that ESM pulls from McAfee ePO.

Before you begin

ePolicy Orchestrator must be running with Policy Auditor.

When selecting the data to show in scorecard, consider the volume of data involved and its effect on performance. Rules are granular and using them results in large amounts of data being displayed. Benchmarks are sets of rules and display one data point for multiple rules.

Task

- 1 Open **Asset Manager** and select the **Scorecard** tab.
All attached McAfee ePO devices are listed.
- 2 For each device, select the data to display - **none**, **benchmarks**, or **benchmarks and rules**.

See also

[How Scorecard view works on page 351](#)


View Policy Auditor data in Scorecard

See Policy Auditor audit results in Asset Manager.

Before you begin

ePO must be installed with Policy Auditor running.

Task

- 1 From the main menu, select **Scorecard**.
The Scorecard view opens.
- 2 To toggle between text view and graph view, click either the hash or bar chart icon.
- 3 To switch the direction of binding, click the dynamic binding icon . By default, benchmark data is bound to assets.
The dynamic binding icon changes to show the direction of the binding.
- 4 To view data for a particular rule, group, or asset, select it.
Data for only the selected rule, group, or asset is shown in the bound table.
- 5 To drill down to a specific rule or asset, click the arrow next to the group name.

See also

[How Scorecard view works on page 351](#)

Configure Scorecard view

Select which benchmarks and benchmark groups are displayed in Scorecard.

Task

- 1 Open Scorecard from the main menu.
- 2 Click the user menu (three vertical dots) on either the **Benchmark Groups** or **Asset Groups** pane.
- 3 Click **Settings**.
- 4 Select the groups and benchmarks you want to display.

See also

[How Scorecard view works on page 351](#)

Configure benchmark groups

Manage the amount of information displayed on the Scorecard by grouping related benchmarks. Expanding and contracting groups gives you context and helps you manage your view of Scorecard data.

Task

- 1 From the main menu, select **Scorecard**.
- 2 Open the user menu (three vertical dots) on the Benchmark Groups pane.
- 3 Create, edit, or delete groups as needed.

See also

[How Scorecard view works on page 351](#)

12

Managing policies and rules

Create, apply, and view policy templates and rules.

Contents

- ▶ *Understanding the Policy Editor*
- ▶ *The Policy Tree*
- ▶ *Manage policies on the Policy Tree*
- ▶ *Set up rule and report for database audit trails*
- ▶ *Normalization*
- ▶ *Rule types and their properties*
- ▶ *Default Policy settings*
- ▶ *Rule operations*
- ▶ *Assign tags to rules or assets*
- ▶ *Modify aggregation settings*
- ▶ *Override action on downloaded rules*
- ▶ *Severity weights*
- ▶ *View policy change history*
- ▶ *Apply policy changes*
- ▶ *Enable Copy Packet*

Understanding the Policy Editor


The **Policy Editor** allows you to create policy templates and customize individual policies.

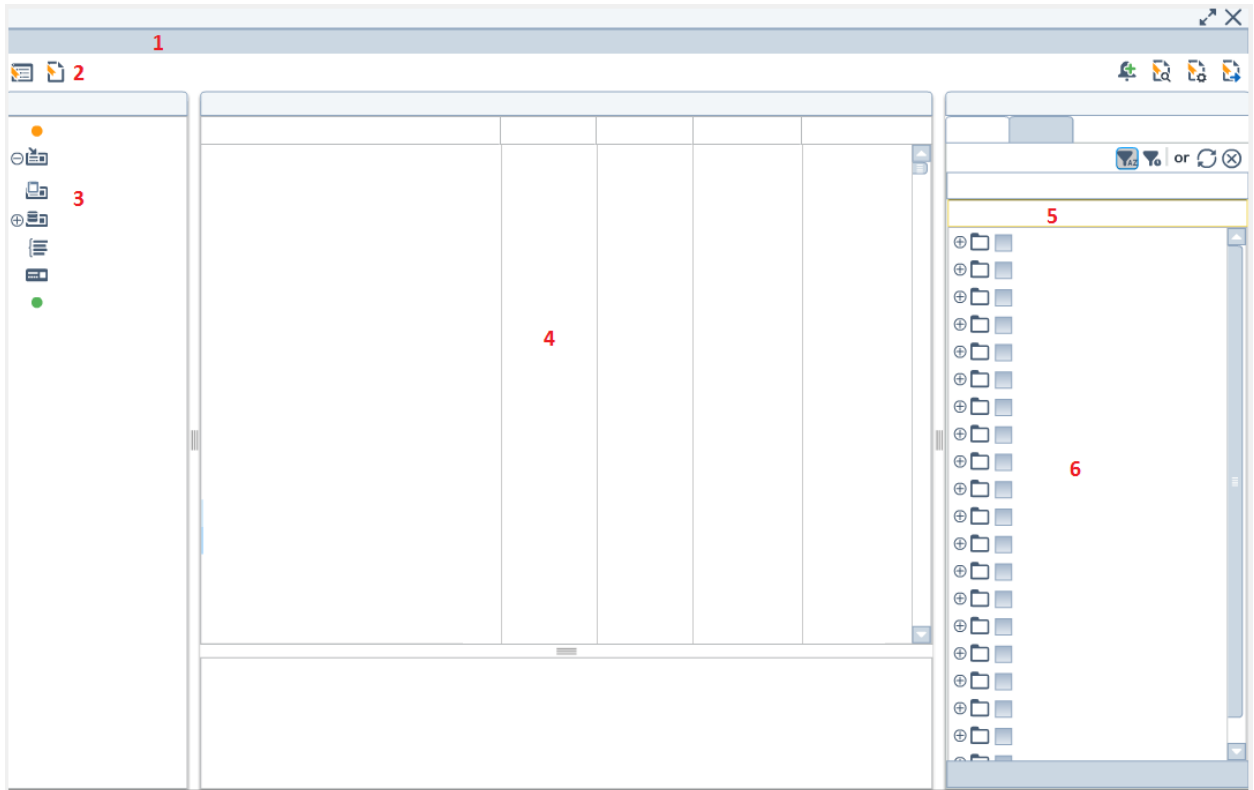
Policy templates, and policy settings on any device, can inherit values from their parents. Inheritance allows policy settings applied to a device to be infinitely configurable while maintaining a level of simplicity and ease-of use. Each policy that is added, with all devices, has an entry in the **Policy Tree**.




When operating in FIPS mode, do not update rules through the rule server. Instead, update them manually (see *Check for rule updates*).

The McAfee rule server maintains all rules, variables, and preprocessors with predefined values or usages. The **Default Policy** inherits its values and settings from these McAfee-maintained settings, and is the ancestor of all other policies. Settings for all other policies and devices inherit their values from the **Default Policy** by default.

To open the editor, click the **Policy Editor** icon, or select the system or device node in the navigation tree. Then, click the **Policy Editor** icon in the actions toolbar .



- | | |
|-------------------------------|------------------------|
| 1 Menu bar | 4 Rule display |
| 2 Bread crumb navigation pane | 5 Tag search field |
| 3 Rule types pane | 6 Filters/Tagging pane |

The types of rules listed in the **Rule Types** pane vary based on the type of device selected in the system navigation tree. The bread crumb navigation pane displays the hierarchy of the policy you have selected. To change the current policy, click the policy's name on the bread crumb navigator pane. Then, click the arrow in the bread crumb navigator pane, which displays the children of the policy. Or, click the **Policy Tree** icon . The menu on the **Policy Tree** lists the things you can do to a policy.

When you select a type in the **Rule Type** pane, all rules of that type are listed in the rule display section. The columns list the specific rule parameters that you can adjust for each rule (except for **Variable** and **Preprocessor**). You can change the settings by clicking the current setting and selecting a new one from the list.

The **Filters/Tagging** pane filters rules displayed in the **Policy Editor**. You can then view only those that meet your criteria, or add tags to the rules to define their functions.

See also

[The Policy Tree on page 357](#)

[Rule types and their properties on page 361](#)

[Manage policies on the Policy Tree on page 357](#)





[Apply policy changes on page 413](#)

The Policy Tree

The **Policy Tree** lists the policies and devices on the system.

The **Policy Tree** allows you to:

- Navigate to view the details of a specific policy or device
- Add a policy to the system
- Change the order of the policies or devices
- Locate any policy or device by name
- Rename, delete, copy, copy and replace, import, or export a policy

Icon	Description
	Policy
	Device is out of sync
	Device is staged
	Device is up to date

See also

[Understanding the Policy Editor on page 355](#)

[Rule types and their properties on page 361](#)

[Manage policies on the Policy Tree on page 357](#)

[Apply policy changes on page 413](#)

Manage policies on the Policy Tree




Manage the policies on the system by taking actions on the **Policy Tree**.


Before you begin




Verify that you have administrator rights or belong to an access group with policy administration permission.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 From the dashboard, click  and select **Policy Editor**.
- 2 On the ESM console, click the **Policy Editor** icon , then click the **Policy Tree** icon .
- 3 Do any of the following:

To...	Do this...
View the rules of a policy	<ul style="list-style-type: none">• Double-click the policy. The rules are listed in the rule display section of the Policy Editor.
Make a policy the child of another	<ul style="list-style-type: none">• Select the child, then drag and drop it on the parent. <div> You can only drag and drop devices onto policies.</div>

To...	Do this...
Locate a policy or device	<ul style="list-style-type: none"> Type the name in the search field.
Add a policy	<ol style="list-style-type: none"> Select the policy that you want to add a policy to, then click the Policy Tree Menu Items icon  . Click New, enter a name for the policy, then click OK.
Rename a policy	<ol style="list-style-type: none"> Select the policy you want to rename, then click the Policy Tree Menu Items icon. Click Rename, enter the new name, then click OK.
Delete a policy	<ol style="list-style-type: none"> Select the policy you want to delete, then click the Policy Tree Menu Items icon. Click Delete, then click OK on the confirmation page.
Copy a policy	<ol style="list-style-type: none"> Select the policy you want to copy, then click the Policy Tree Menu Items icon. Click Copy, enter a name for the new policy, then click OK.
Move devices to a policy	<ol style="list-style-type: none"> Select the devices that you need to move, then click the Policy Tree Menu Items icon  . Highlight Move, then select the policy you want to move the devices to.
Copy and replace a policy	<ol style="list-style-type: none"> Select the policy you want to copy, click the Policy Tree Menu Items icon, then select Copy and Replace. In Select Policy, select the policy you want to replace. Click OK, then click Yes. <p>The settings of the policy you copied are applied to the policy you replaced, but the name remains the same.</p>
Import a policy	<p>The import occurs from the currently selected device down.</p> <ol style="list-style-type: none"> Select the level on the tree where you want to import the new policy, click the Policy Tree Menu Items icon, then select Import. Browse to and upload the file you want to import. <div style="display: flex; align-items: center;">  <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> If an error message appears, see <i>Troubleshoot Import Policy</i> for a solution. </div> </div> <ol style="list-style-type: none"> Select the import options that you want to use, then click OK.
Export a policy	<ol style="list-style-type: none"> Select the policy that you want to export. The export includes the selected node and up in the hierarchy. Only standard rules with custom settings or custom rules are exported, so at least one of these must be selected for the Export option to enable. Click Menu, then select Export. Select the export options you want to use, click OK, then select the location to save the exported policy file.


- 4 To close the **Policy Tree**, double-click a policy or device, or click the close icon .

Table 12-1 Option definitions

Option	Definition
Menu bar	Run your cursor over an item on this bar and select any of the options available. Options change based on the rule type or rule selected.
Bread crumb navigation bar	The Policy Tree icon opens the list of all policies on the ESM. The bread crumb list shows which policy you are working on.
Rule Types pane	Click on any of the rule types in this pane to view the rules of that type in the rules display pane.
Rule display pane	Click on a rule to view its description at the bottom of the pane or perform any of the actions available for it on the menu bar or in the columns of the rule display pane.
Tag search field	Type the name of a tag you are searching for, then select a tag from the list of possible matches.
Filters/Tagging pane	On the Filter tab, sort the rules in the rule display pane in alphabetical order or by time, as well as filter the list so you can view only those rules that meet the criteria you select. On the Tags tab, add tags to selected rules in the rule display pane so you can filter rules by their tags. You can add, edit, and remove custom tags and tag categories.
Create Alarm icon	Add an alarm so you are notified when an event is generated by the rule you select.
Severity Weights icon	Set the severity for assets, tags, rules, and vulnerabilities so they can be used when calculating event severity.
View Policy Change History icon	View and export a list of the changes that have been made to the current policy.
Settings icon	Define settings for alerts only mode and oversubscription mode, update the rules from the McAfee server, and view the summary of the update status of the devices on the policy tree.
Rollout icon	Rollout policy changes to the ESM.

Table 12-2 Option definitions

Option	Definition
Overwrite selected policy (name excluded)	Select to import the policy settings into the currently selected item in the policy tree. If importing multiple policies, the first policy overwrites the selected policy and all subsequent policies are inserted as children of the current node, leaving their hierarchical relationship intact. This option doesn't change the name of the selected policy.
Insert as child policy of selected policy	Select to import the policy as a child of the currently selected item in the policy tree. If importing multiple policies, all policies are inserted as children to the current node, leaving their hierarchical relationship intact.
Overwrite existing rules	Select to delete the existing rule and overwrite it with the rule that is part of the policy being imported.
Create a new rule when a conflict exists	Select to keep both of the rules, creating a new ID for the imported rule.
Skip the rule when an existing rule exists	Select to keep the existing rule and will not import the conflicting rule.
Import Policy	Click to begin importing the policy.

Table 12-3 Option definitions

Option	Definition
Export Method Settings	Select whether you want custom rules and variables to be included as part of this export. Due to the possible dependency of custom rules on custom variables, custom rules cannot be exported without also exporting the custom variables. Select the custom rules and variables option that best suits the desired action for the current export.
Advanced Options	Click to select the policy levels to be exported.
Export current policy	Select to export the policy with all its hierarchy. It is flattened, which means the settings are compressed down into one level of policy, with the most immediate policy's settings taking precedence on an item by item basis. For example, if you have a device selected, both policies above the selected policy are exported. You have to select a child if you want the parent of that child exported. Also, the settings of the selected policy have precedence over the parent policy settings when the file is compressed down into one level of policy.
Current policy with no settings from parent policy	Select to export only the selected policy's settings.
Current policy including parent policies	Select to export the selected policy and all of its parents, with the hierarchical structure kept intact.

See also
[Understanding the Policy Editor on page 355](#)
[The Policy Tree on page 357](#)
[Rule types and their properties on page 361](#)
[Apply policy changes on page 413](#)


Set up rule and report for database audit trails

A **Privileged User Audit Trails** report allows you to view the audit trail for modifications made to the database or to track access to a database or table that was associated with a specific database event.

After the parameters for generating this report are set up, you receive compliance report notifications that display the audit trail associated with each event. To generate the audit trail events, you must add a **Data Access** rule and a **Privileged User Audit Trails** report.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select **DEM | Data Access**.
- 2 Highlight **DEM - Template Rule - Trusted Use Access From IP Range** in the rules display pane.
- 3 Click **Edit | Copy**, then click **Edit | Paste**.
- 4 Change the name and properties of the new rule.
 - a Highlight the new rule, then select **Edit | Modify**.
 - b Enter a name for the rule, then type the user name.
 - c Select the **Untrusted** action type, then click **OK**.
- 5 Click the **Rollout** icon .

- 6 Set up the report:
 - a On **System Properties**, click **Reports | Add**.
 - b Fill in sections 1 – 3, and 6.
 - c In section 4, select **Report PDF** or **Report HTML**.
 - d In section 5, select **Compliance | SOX | Privileged User Audit Trails (Database)**.
 - e Click **Save**.
- 7 To generate the report, click **Run Now**.

Normalization

Rules are named and described by each vendor. As a result, the same type of rule often has different names, making it difficult to gather information for the types of events that are occurring.

McAfee compiled, and continually updates, a list of normalized IDs that describe rules so that events can be grouped into useful categories. When you click **Normalization** in the **Rule Types** pane of the **Policy Editor**, these IDs, names, and descriptions are listed.

These event features offer the option to organize event information using normalized IDs:

- View component fields — **Normalized Event Summary** is an option when defining fields for an event query in the pie chart, bar chart, and list components (see *Manage a query*).
- View component filters — When you are creating a new view, you can select to filter event data on a component by the normalized IDs (see *Manage a query*).
- View filters — **Normalized ID** is an option on the list of view filters (see *Filtering views*).
- View list — A **Normalized Event Summary** view is available on the list of **Event Views**.

The **Details** tab on the **Event Analysis** view lists the normalization ID for the events that appear on the list.

When you are adding **Normalized ID** filters to a new or existing view, you can:






- Filter by all the normalized IDs in a first-level folder. A mask (/5 for a first-level folder) is included at the end of the ID to indicate that the events will also be filtered by the child IDs of the selected folder.
- Filter by the IDs in a second- or third-level folder. A mask (/12 for a second-level folder, /18 for a third-level folder) is included at the end of the ID to indicate that the events are filtered by the child IDs of the selected subfolder. The fourth level doesn't have a mask.
- Filter by a single ID.
- Filter by multiple folders or IDs at one time using the **Ctrl** or **Shift keys** to select them.

Rule types and their properties

The **Rule Types** pane of the **Policy Editor** page allows you to access all rules by type.


You can import, export, add, edit, and perform various operations on a rule once it is selected. The functions that you can perform are limited by the type of rule.

All rules are based on a hierarchy system in which each rule inherits its usage from its parent. The rule (except for **Variable** and **Preprocessor** rules) is marked with an icon to indicate where it inherits its usage. The icon has a dot on the lower-left corner if the inheritance chain broke somewhere below the current row.

Icon	Description
	The parent's setting determined the usage for this item. Most rules are set to inherit by default, but the usage can be changed.
	Indicates that the inheritance chain is broken at this level and the inheritance value is turned off.
	The current rule usage is used when the inheritance chain is broken.
	Indicates that the inheritance chain is broken at this level. Items below this point do not inherit any further up the chain. This setting is useful to force rules to use their default.
	Indicates a custom value; you set the value to something other than the default.

Properties

When a rule type is selected, the rule display pane shows all rules of that type on the system and their property settings. These properties can include **Action**, **Severity**, **Blacklist**, **Aggregation**, and **Copy Packet**.

This property...	Allows you to...
Action	Set the action performed by this rule. The available options are based on the type of rule.  Blacklist items can't move on to their destination; if Pass is selected in the Blacklist column, the system automatically changes it to Alert .
Severity	Select the severity of the rule part when the rule is triggered. Severity is based on 1–100, with 100 being the most severe.
Blacklist	Auto-create a blacklist entry on a per rule basis when the rule is triggered on the device. You can choose whether to blacklist only the IP address or the IP address and port.
Aggregation	Set per rule aggregation for events that are created when a rule is triggered. The aggregation settings defined on the Event Aggregation pages (see <i>Aggregate events or flows</i>) apply only to those rules that are set in the Policy Editor.
Copy Packet	Copy packet data to the ESM, which is useful in the event of lost communication. If there is a copy of the packet data, you can access the information by retrieving the copy.

Change these settings by clicking the current setting and selecting another.

See also

[Understanding the Policy Editor on page 355](#)

[The Policy Tree on page 357](#)

[Manage policies on the Policy Tree on page 357](#)

[Apply policy changes on page 413](#)

ADM rules

McAfee ADM is a series of network appliances powered by the ICE Deep Packet Inspection (DPI) Engine.

The ICE Engine is a software library and collection of protocol and content plug-in modules that can identify and extract content from raw network traffic in real time. It can fully reassemble and decode application level content, transforming cryptic network packet streams into easily readable content as if it were being read from a local file.

The ICE engine is capable of automatically identifying protocols and content types without the need to rely on fixed TCP port numbers or file extensions. ICE engine does not rely on signatures to perform its analysis and decoding, instead its modules implement full parsers for each protocol or content type. This results in

extremely accurate identification and decoding of content and allows content to be identified and extracted even when that content is compressed or otherwise encoded and, therefore, doesn't pass over the network in clear text.

As a result of this highly accurate identification and decoding, the ICE engine is able to offer a uniquely deep view of network traffic. For example, the ICE engine could receive a PDF document stream that traversed the network inside a .zip file, as a BASE-64 encoded attachment to an SMTP email from a SOCKS proxy server.

This application and document-awareness allow the ADM to provide invaluable security context. It can detect threats that can't be easily detected by a traditional IDS or IPS, such as:

- Leak of sensitive information and documents or communication policy violations.
- Unauthorized application traffic (for example, who's using Gnutella?).
- Applications being used in unexpected ways (for example, HTTPS on non-standard port).
- Potentially malicious documents (for example, document does not match its extension).
- New generation of exploits (for example, PDF document with an embedded executable).

The ADM also detects malicious traffic patterns by detecting anomalies in application and transport protocols (for example, an RPC connection is malformed or TCP destination port is 0).

Supported applications and protocols

There are more than 500 supported applications and protocols in which ADM can monitor, decode, and detect anomalies. Here is a sample list:

- Low-level network protocols — TCP/IP, UDP, RTP, RPC, SOCKS, DNS, and others
- Email — MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- Chat — MSN, AIM/Oscar, Yahoo, Jabber, IRC
- Webmail — AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook, and MySpace email
- P2P — Gnutella, bitTorrent
- Shell — SSH (detection only), Telnet
- Instant messaging — AOL, ICQ, Jabber, MSN, SIP, and Yahoo
- File transfer protocols — FTP, HTTP, SMB, and SSL
- Compression and extraction protocols — BASE64, GZIP, MIME, TAR, ZIP, and others
- Archive files — RAR Archives, ZIP, BZIP, GZIP, Binhex, and UU-encoded archives
- Installation packages — Linux packages, InstallShield cabinets, Microsoft cabinets
- Image files — GIFs, JPEGs, PNGs, TIFFs, AutoCAD, Photoshop, Bitmaps, Visio, Digital RAW, and Windows icons
- Audio files — WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast, and more
- Video files — AVI, Flash, QuickTime, Real Media, MPEG-4, Vivo, Digital Video (DV), Motion JPEG, and more
- Other applications and files — Databases, spreadsheets, faxes, web applications, fonts, executable files, Microsoft Office applications, games, and even software development tools
- Other protocols — Network printer, shell access, VoIP, and peer-to-peer

Key concepts

Key to understanding how ADM works is an awareness of the following concepts:

- **Object** — An object is an individual item of content. An email is an object but also an object container since it has a message body (or two) and attachments. An HTML page is an object which may contain additional objects such as images. A .zip file and each file within the .zip file are all objects. ADM unpacks the container and treats each object inside as its own object.
- **Transaction** — A transaction is a wrapper around the transfer of an object (content). A transaction contains at least one object; however, if that object is a container, like a .zip file, then the single transaction might contain several objects.
- **Flow** — A flow is the TCP or UDP network connection. A flow might contain many transactions.

Manage custom ADM, DEM, or correlation rules

Copy a predefined rule and use it as a template for a custom rule. When you add a custom rule, you can edit the settings, copy and paste it to use it as a template for a new custom rule, or delete it.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the **Policy Editor**, select **ADM** or **DEM** | **Database, Data Access**, or **Transaction Tracking**.
- 2 Do any of the following:

To...	Do this...
View all custom ADM or DEM rules	<ol style="list-style-type: none"> 1 Select the Filter tab in the Filters/Tagging pane. 2 Click the Advanced bar at the bottom of the pane. 3 In the Origin field, select user-defined. 4 Click Run Query. <p>The custom rules of the type you select are listed in the rule display pane.</p>
Copy and paste a rule	<ol style="list-style-type: none"> 1 Select a predefined or custom rule. 2 Click Edit Copy 3 Click Edit Paste. <p>The rule you copied is added to the list of existing rules, with the same name.</p> <ol style="list-style-type: none"> 4 To change the name, click Edit Modify.
Modify a custom rule	<ol style="list-style-type: none"> 1 Select the custom rule. 2 Click Edit Modify.
Delete a custom rule	<ol style="list-style-type: none"> 1 Select the custom rule. 2 Click Edit Delete.

Add custom ADM, database, or correlation rules

In addition to using the predefined ADM, Database, or Correlation rules, you can create complex rules using logical and regular expressions. The editors you use to add these different rule types are very similar to each other so they are described in the same sections.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select **ADM, DEM | Database**, or **Correlation**.
- 2 Click **New**, then select the rule type you are adding.
- 3 Enter the information requested, then drag-and-drop logical elements and expression components from the toolbar to the **Expression Logic** area to build the rule's logic.
- 4 Click **OK**.

Table 12-4 Option definitions



Option	Definition
Name	Type a descriptive name for the rule.
Severity	Select a severity setting.
Normalization ID	Change the default normalized ID.
Tags	Select tags that define the categories that the rule belongs to.
Type	Select the type of database rule this is.
Default Action	Select the alert action that is triggered by this rule.  Actions can be added to the list of default actions (see <i>Add a DEM action</i>).
Expression Logic area	Drag and drop logical elements and components in this area to set the logic for the rule.
AND, OR logical elements	Drag and drop them in the Expression Logic area to set the logic for the rule.
Expression Component icon 	Drag and drop the icon to define the details for the logical elements.
Description	Type a description of the rule, which will appear in the description area of the Policy Editor when you select it.

Table 12-5 Option definitions


Option	Definition
Name	Type a descriptive name for the rule.
Severity	Select a severity setting.
Normalization ID	Change the default normalized ID.
Tags	Select tags that define the categories that the rule belongs to.
Type	Select the type of database rule this is.
Default Action	Select the alert action that is triggered by this rule.  Actions can be added to the list of default actions (see <i>Add a DEM action</i>).
Expression Logic area	Drag and drop logical elements and components in this area to set the logic for the rule.
AND, OR logical elements	Drag and drop them in the Expression Logic area to set the logic for the rule.

Table 12-5 Option definitions *(continued)*


Option	Definition
Expression Component icon 	Drag and drop the icon to define the details for the logical elements.
Description	Type a description of the rule, which will appear in the description area of the Policy Editor when you select it.

Table 12-6 Option definitions

Option	Definition
Name	Type a descriptive name for the rule.
Severity	Select a severity setting.
Normalization ID	Change the default normalized ID.
Tags	Select tags that define the categories that the rule belongs to.
Group By	Create a list of fields that events can be grouped by when they come in to the correlation engine.
Correlation Logic area	Drag and drop logical elements and components in this area to set the logic for the rule (see <i>Example of custom correlation rule</i>).
Parameters	Customize instances of a rule and component reuse (see <i>Add parameters to a correlation rule or component</i>).
AND, OR, SET logical elements	Drag and drop them in the Correlation Logic area to set the logic for the rule.
Match Component, Deviation Component, Rules/Components icons	Drag and drop components to define the details for the logical elements.
Description	Add a description of the rule, which will appear in the description area of the Policy Editor when you click it.

Table 12-7 Option definitions

Option	Definition
Events, Flows	Select the type of data that you want the filters applied to. You can select both.
Add	Add the filters for this component.
Advanced Options A number of Distinct Values...	Select if a specific number of values must occur in a specific field before the component triggers. <ul style="list-style-type: none"> • Distinct Values — Click the Default Value icon ☆ to select the number of values that must occur. • Monitored field — Click the Default Value icon ☆ to select the field that the values must occur in.
This component should only trigger if...	Select to have the component trigger only if matches do not occur in the time specified in the Time Window field at the gate level.
Override Group By	Select to customize the grouping of the events in a correlation rule. If you have a rule that groups by a specific field, you can override one of its components to match on a field that you specify on the Configure Group By overrides page. Click Configure to set the override field (see <i>Override Group by</i>).

Table 12-8 Option definitions


Option	Definition
Not	Select to exclude the values you select.
Term	(ADM and DEM) Select the metric reference for this expression. For a description of the options for a DEM database rule, see <i>DEM rule metric references</i> .
Description	(ADM) Type a description of the component.
Dictionary	(ADM) If you want this rule to reference an ADM dictionary that is on the ESM, select it on the drop-down list (see <i>ADM dictionaries</i>).
Operator	<p>Select the relational operator.</p> <p>ADM</p> <ul style="list-style-type: none"> • Equal to = • Not equal to != • Greater than > • Greater than equal to >= • Less than equal to <= • Less than < <p>DEM Database</p> <ul style="list-style-type: none"> • EQ - Equal to • BT - Between • GE - Greater than equal to • GT - Greater than • LE - Less than equal to • LT - Less than • NB - Not between • NE - Not equal to • NGT - Not greater than • NLE - Not less than • REGEXP - Regular expression
Match values	Select whether the rule triggers when any of the values match the pattern you define, or only if all the values match the pattern.
Value	<p>(ADM) Select the variables to filter by.</p> <ul style="list-style-type: none"> • If the variables icon is next to the field, click it and select the variables. • If there is no icon, type the value following the instructions in the Valid Input field. <p>(DEM) Enter the value to filter by.</p>
Valid Input	View hints for the values that you can enter in the Value field.

Edit logical elements

The AND, OR, and SET logical elements have default settings. These can be changed on the **Edit Logic Element** page.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the rule editor, drag-and-drop a logic element in the **Expression Logic** or **Correlation Logic** area.
- 2 Click the **Menu** icon  for the element you want to edit, then click **Edit**.
- 3 Change the settings, then click **OK**.

See also

[Logic elements on page 264](#)

ADM rules syntax

The ADM rules are very similar to C expressions.

The main difference is a more extensive set of literals (numbers, strings, regular expressions, IP addresses, MAC addresses, and Booleans). String terms can be compared with string and Regex literals to test their content but they can also be compared with numbers to test their length. Numeric, IP address, and MAC address terms can only be compared with the same type of literal value. The only exception is that everything can be treated as a Boolean to test for its existence. Some terms can have multiple values, for example the following rule would trigger for PDF files inside .zip files: `type == application/zip && type == application/pdf`.

Table 12-9 Operators

Operator	Description	Example
&&	Logical AND	<code>protocol == http && type == image/gif</code>
	Logical OR	<code>time.hour < 8 time.hour > 18</code>
^^	Logical XOR	<code>email.from == "a@b.com" ^^ email.to == "a@b.com"</code>
!	Unary NOT	<code>!(protocol == http protocol == ftp)</code>
==	Equal	<code>type == application/pdf</code>
!=	Not equal	<code>srcip != 192.168.0.0/16</code>
>	Greater	<code>objectsize > 100M</code>
>=	Greater or equal	<code>time.weekday >= 1</code>
<	Less	<code>objectsize < 10K</code>
<=	Less or equal	<code>time.hour <= 6</code>

Table 12-10 Literals

Literal	Example
Number	1234, 0x1234, 0777, 16K, 10M, 2G
String	"a string"
Regex	/[A-Z] [a-z]+/
IPv4	1.2.3.4, 192.168.0.0/16, 192.168.1.0/255.255.255.0
MAC	aa:bb:cc:dd:ee:ff
Bool	true, false

Table 12-11 Type operator compatibility

Type	Operators	Notes
Number	<code>==, !=, >, >=, <, <=</code>	
String	<code>==, !=</code>	Compare content of string with String/Regex
String	<code>>, >=, <, <=</code>	Compare length of string
IPv4	<code>==, !=</code>	
MAC	<code>==, !=</code>	
Bool	<code>==, !=</code>	Compare against true/false, also supports implied comparison with true, for example the following tests whether the email.bcc term occurs: <code>email.bcc</code>

Table 12-12 ADM regex grammar

Basic operators	
	Alternation (or)
*	Zero or more
+	One or more
?	Zero or one
()	Grouping (a b)
{ }	Repeating Range {x} or {,x} or {x,} or {x,y}
[]	Range [0-9a-z] [abc]
[^]	Exclusive Range [^abc] [^0-9]
.	Any Character
\	Escape Character
Escapes	
\d	Digit [0-9]
\D	Non-Digit [^0-9]
\e	Escape (0x1B)
\f	Form Feed (0x0C)
\n	Line Feed (0x0A)
\r	Carriage Return (0x0D)
\s	White Space
\S	Not White Space
\t	Tab (0x09)
\v	Vertical Tab (0x0B)
\w	Word [A-Za-z0-9_]
\W	Not Word
\x00	Hex Representation
\0000	Octal Representation
^	Start of line
\$	End of line
	The start of line and end of line anchors (^ and \$) don't work for objcontent.

POSIX character classes	
[[:alnum:]]	Digits and letters
[[:alpha:]]	All letters
[[:ascii:]]	ASCII Characters
[[:blank:]]	Space and tab
[[:cntrl:]]	Control characters
[[:digit:]]	Digits
[[:graph:]]	Visible characters
[[:lower:]]	Lowercase letters
[[:print:]]	Visible characters and spaces
[[:punct:]]	Punctuation and Symbols
[[:space:]]	All whitespace characters
[[:upper:]]	Uppercase characters
[[:word:]]	Word characters
[[:xdigit:]]	Hexadecimal Digit

See also

[ADM rule reference material on page 124](#)

[ADM rule term types on page 127](#)

[ADM rule metric references on page 129](#)

[Protocol-specific properties on page 131](#)

[Protocol anomalies on page 132](#)

ADM dictionary examples

The ADM engine can match object content or any other metric or property with a single column dictionary for true or false (exists in the dictionary or does not exist in the dictionary).

Table 12-13 Single column dictionary examples

Type of dictionary	Example
String dictionary with common spam words	<p>"Cialis"</p> <p>"cialis"</p> <p>"Viagra"</p> <p>"viagra"</p> <p>"adult web"</p> <p>"Adult web"</p> <p>"act now! don't hesitate!"</p>
Regular expression dictionary for authorization key words	<p>/(\password passwd pwd)[^a-z0-9]{1,3}(admin login password user)/i</p> <p>/(customer client)[^a-z0-9]{1,3}account[^a-z0-9]{1,3}number/i</p> <p>/fund[^a-z0-9]{1,3}transaction/i</p> <p>/fund[^a-z0-9]{1,3}transfer[^a-z0-9]{1,3}[0-9,.,]+/i</p>

Table 12-13 Single column dictionary examples *(continued)*

Type of dictionary	Example
String dictionary containing hash values for known bad executables	"fec72ceae15b6f60cbf269f99b9888e9" "fed472c13c1db095c4cb0fc54ed28485" "feddedb607468465f9428a59eb5ee22a" "ff3cb87742f9b56dfdb9a49b31c1743c" "ff45e471aa68c9e2b6d62a82bbb6a82a" "ff669082faf0b5b976cec8027833791c" "ff7025e261bd09250346bc9efdfc6c7c"
IP addresses of critical assets	192.168.1.12 192.168.2.0/24 192.168.3.0/255.255.255.0 192.168.4.32/27 192.168.5.144/255.255.255.240

Table 12-14 Double column dictionary examples

Type of dictionary	Example
String dictionary with common spam words and categories	"Cialis" "pharmaceutical" "cialis" "pharmaceutical" "Viagra" "pharmaceutical" "viagra" "pharmaceutical" "adult web" "adult" "Adult web" "adult" "act now! don't hesitate!" "scam"
Regular expression dictionary for authorization key words and categories	/((password passwd pwd)[^a-z0-9]{1,3}(admin login password user)/i "credentials" /(customer client)[^a-z0-9]{1,3}account[^a-z0-9]{1,3}number/i "pii" /fund[^a-z0-9]{1,3}transaction/i "sox" /fund[^a-z0-9]{1,3}transfer[^a-z0-9]{1,3}[0-9,.]+/i "sox"

Table 12-14 Double column dictionary examples *(continued)*

Type of dictionary	Example
String dictionary containing hash values for known bad executables and categories	"fec72ceae15b6f60cbf269f99b9888e9" "Trojan" "fed472c13c1db095c4cb0fc54ed28485" "Malware" "feddedb607468465f9428a59eb5ee22a" "Virus" "ff3cb87742f9b56dfdb9a49b31c1743c" "Malware" "ff45e471aa68c9e2b6d62a82bbb6a82a" "Adware" "ff669082faf0b5b976cec8027833791c" "Trojan" "ff7025e261bd09250346bc9efdfc6c7c" "Virus"
IP addresses of critical assets & groups	192.168.1.12 "Critical Assets" 192.168.2.0/24 "LAN" 192.168.3.0/255.255.255.0 "LAN" 192.168.4.32/27 "DMZ" 192.168.5.144/255.255.255.240 "Critical Assets"

See also

[Application Data Monitor \(ADM\) dictionaries on page 119](#)

[Setting up an ADM dictionary on page 120](#)

[Manage ADM dictionaries on page 123](#)

[Reference an ADM dictionary on page 121](#)


ADM rule term types

All terms in an ADM rule have a specific type.

Each term is either an IP address, a MAC address, a number, a string, or a boolean. In addition there are two extra literal types: regular expressions and lists. A term of a specific type can generally only be compared against a literal of the same type or a list of literals of the same type (or a list of lists of ...). There are three exceptions to this rule:

- 1 A string term can be compared against a numeric literal to test its length. The following rule triggers if a password is fewer than eight characters long (password is a string term): password < 8
- 2 A string term can be compared against a regular expression. The following rule triggers if a password only contains lower case letters: password == /^[a-z]+\$
- 3 All terms can be tested against boolean literals to test whether they occur at all. The following rule triggers if an email has a CC address (email.cc is a string term): email.cc == true

Type	Format description
IP addresses	<ul style="list-style-type: none"> • IP address literals are written in standard dotted-quad notation, they are not enclosed in quotes: 192.168.1.1 • IP addresses can have a mask written in standard CIDR notation, there must not be any white space between the address and the mask: 192.168.1.0/24 • IP addresses can also have masks written out in long form: 192.168.1.0/255.255.255.0
Mac addresses	<ul style="list-style-type: none"> • MAC address literals are written using standard notation, as with IP addresses, they are not enclosed in quotes: aa:bb:cc:dd:ee:ff

Type	Format description
Numbers	<ul style="list-style-type: none"> • All numbers in ADM rules are 32-bit integers. They can be written in decimal: 1234 • They can be written in hexadecimal: 0xabcd • They can be written in octal: 0777 • They can have a multiplier appended to multiply by 1024 (K), 1048576 (M) or 1073741824 (G): 10M
Strings	<ul style="list-style-type: none"> • Strings are enclosed in double quotes: "this is a string" • Strings can use standard C escape sequences: "\tThis is a \"string\" containing\x20escape sequences\n" • When comparing a term against a string, the whole term must match the string. If an email message has a from address of someone@somewhere.com then the following rule will not trigger: email.from == "@somewhere.com" • To match only a part of a term, a regular expression literal should be used instead. String literals must be used when possible because they are more efficient. <div>  All email address and URL terms are normalized before matching so it is not necessary to take account of things like comments within email addresses. </div>
Booleans	<ul style="list-style-type: none"> • The boolean literals are true and false.

Type	Format description
Regular expressions	<ul style="list-style-type: none"> Regular expression literals use the same notation as languages like Javascript and Perl, enclosing the regular expression in forward slashes: <code>/[a-z]+/</code> Regular expressions can be followed by standard modifier flags, though "i" is the only one currently recognized (case-insensitive): <code>/[a-z]+/i</code> Regular expression literals should use the POSIX Extended syntax. Currently Perl extensions work for all terms except the content term but this might change in future versions. When comparing a term against a regular expression, the regular expression matches any substring within the term unless anchor operators are applied within the regular expression. The following rule triggers if an email is seen with an address of "someone@somewhere.com": <code>email.from == /@somewhere.com/</code>
Lists	<ul style="list-style-type: none"> List literals consist of one or more literals enclosed in square brackets and separated by commas: <code>[1, 2, 3, 4, 5]</code> Lists might contain any kind of literal, including other lists: <code>[192.168.1.1, [10.0.0.0/8, 172.16.128.0/24]]</code> Lists must only contain one kind of literal, it's not valid to mix strings and numbers, strings and regular expressions, IP addresses and MAC addresses. When a list is used with any relational operator other than not-equal (<code>!=</code>), then the expression is true if the term matches any literal in the list. The following rule triggers if the source IP address matches any of the IP addresses in the list: <code>srcip == [192.168.1.1, 192.168.1.2, 192.168.1.3]</code> It is equivalent to: <code>srcip == 192.168.1.1 srcip == 192.168.1.2 srcip == 192.168.1.3</code> When used with the not-equal (<code>!=</code>) operator, the expression is true if the term doesn't match all of the literals in the list. The following rule triggers if the source IP address is not 192.168.1.1 or 192.168.1.2: <code>srcip != [192.168.1.1, 192.168.1.2]</code> It is equivalent to: <code>srcip != 192.168.1.1 && srcip != 192.168.1.2</code> Lists might also be used with the other relational operators, though it doesn't make a lot of sense. The following rule triggers if the object size is greater than 100 or if the object size is greater than 200: <code>objectsize > [100, 200]</code> It is equivalent to: <code>objectsize > 100 objectsize > 200</code>

See also[ADM rule reference material on page 124](#)[ADM rules syntax on page 124](#)[ADM rule metric references on page 129](#)[Protocol-specific properties on page 131](#)[Protocol anomalies on page 132](#)**ADM rule metric references**

Here are lists of metric references for ADM rule expressions, which are available on the **Expression Component** page when you are adding an ADM rule.

For Common Properties and Common Anomalies, the parameter-type value you can enter for each one is shown in parentheses after the metric reference.

Common Properties

Property or term	Description
Protocol (Number)	The application protocol (HTTP, FTP, SMTP)
Object Content (String)	The content of an object (text inside a document, email message, chat message). Content matching is not available for binary data. Binary objects can, however, be detected using Object Type (objtype)
Object Type (Number)	Specifies the type of the content as determined by ADM (Office Documents, Messages, Videos, Audio, Images, Archives, Executables)
Object Size (Number)	Size of the object. Numeric multipliers K, M, G can be added after the number (10K, 10M, 10G)
Object Hash (String)	The hash of the content (currently MD5)
Object Source IP Address (Number)	The source IP address of the content. IP address can be specified as 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Object Destination IP Address (Number)	The destination IP address of the content. IP address can be specified as, 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Object Source Port (Number)	The source TCP/UDP port of the content
Object Destination Port (Number)	The destination TCP/UDP port of the content
Object Source IP v6 Address (Number)	The source IPv6 address of the content
Object Destination IPv6 Address (Number)	The destination IPv6 address of the content
Object Source MAC Address (mac name)	The source MAC address of the content (aa:bb:cc:dd:ee:ff)
Object Destination MAC Address (mac name)	The destination MAC address of the content (aa:bb:cc:dd:ee:ff)
Flow Source IP Address (IPv4)	Source IP address of the flow. IP address can be specified as 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Flow Destination IP Address (IPv4)	Destination IP address of the flow. IP address can be specified as 192.168.1.1, 192.168.1.0/24, 192.168.1.0/255.255.255.0
Flow Source Port (Number)	Source TCP/UDP port of flow
Flow Destination Port (Number)	Destination TCP/UDP port of flow
Flow Source IPv6 Address (Number)	Source IPv6 address of the flow
Flow Destination IPv6 Address (Number)	Destination IPv6 address of the flow
Flow Source MAC Address (mac name)	Source MAC address of the flow
Flow Destination MAC Address (mac name)	Destination MAC address of flow
VLAN (Number)	Virtual LAN ID
Day of Week (Number)	The day of the week. Valid values are 1–7; 1 is Monday.
Hour of Day (Number)	The hour of the day set to GMT. Valid values are 0–23.
Declared Content Type (String)	Type of the content as specified by the server. In theory, Object Type (objtype) is always the actual type and Declared Content-type (content-type) is not trustworthy because it can be spoofed by the server/application.
Password (String)	Password used by the application for authentication.
URL (String)	Website URL. Applies only to HTTP protocol.

Property or term	Description
File Name (String)	Name of the file being transferred.
Display Name (String)	
Host Name (String)	Host name as specified in DNS lookup.

Common Anomalies

- User logged off (Boolean)
- Authorization error (Boolean)
- Authorization successful (Boolean)
- Authorization failed (Boolean)

See also

[ADM rule reference material on page 124](#)

[ADM rules syntax on page 124](#)

[ADM rule term types on page 127](#)

[Protocol-specific properties on page 131](#)

[Protocol anomalies on page 132](#)

Protocol-specific properties

In addition to providing properties that are common across most protocols, ADM also provides protocol-specific properties that can be used with ADM rules. All protocol-specific properties are also available in the **Expression Component** page when adding an ADM rule.

Examples of protocol-specific properties

These properties apply to these tables:

```
*   Detection only
**  No decryption, captures X.509 certificates and encrypted data
*** Via RFC822 module
```

Table 12-15 File transfer protocol modules

FTP	HTTP	SMB*	SSL**
Display Name	Display Name	Display Name	Display Name
File Name	File Name	File Name	File Name
Host Name	Host Name	Host Name	Host Name
URL	Referer		
	URL		
	All HTTP headers		

Table 12-16 Email protocol modules

DeltaSync	MAPI	NNTP	POP3	SMTP
Bcc***	Bcc	Bcc***	Bcc***	Bcc***
Cc***	Cc	Cc***	Cc***	Cc***
Display Name	Display Name	Display Name	Display Name	Display Name
From***	From	From***	From***	From***
Host Name	Host Name	Host Name	Host Name	Host Name
Subject***	Subject	Subject***	Subject***	To***
To***	To	To***	To***	Subject***
	User Name		User Name	

Table 12-17 Webmail protocol modules

AOL	Gmail	Hotmail	Yahoo
Attachment Name	Attachment Name	Attachment Name	Attachment Name
Bcc***	Bcc***	Bcc***	Bcc***
Cc***	Cc***	Cc***	Cc***
Display Name	Display Name	Display Name	Display Name
File Name	File Name	File Name	File Name
Host Name	Host Name	Host Name	Host Name
From***	From***	From***	From***
Subject***	Subject***	Subject***	Subject***
To***	To***	To***	To***

See also[ADM rule reference material on page 124](#)[ADM rules syntax on page 124](#)[ADM rule term types on page 127](#)[ADM rule metric references on page 129](#)[Protocol anomalies on page 132](#)**Protocol anomalies**

Beyond the common properties and protocol-specific properties, ADM also detects hundreds of anomalies in low-level, transport, and application protocols. All protocol anomaly properties are of type Boolean and are available in the **Expression Component** page when you are adding an ADM rule.

Table 12-18 IP

Term	Description
ip.too-small	IP packet is too small to contain a valid header.
ip.bad-offset	IP data offset goes past end of packet.
ip.fragmented	IP packet is fragmented.
ip.bad-checksum	IP packet checksum doesn't match data.
ip.bad-length	IP packet totlen field goes past end of packet.

Table 12-19 TCP

Term	Description
tcp.too-small	TCP packet is too small to contain a valid header.
tcp.bad-offset	TCP packet's data offset goes past end of packet.
tcp.unexpected-fin	TCP FIN flag set in non-established state.
tcp.unexpected-syn	TCP SYN flag set in established state.
tcp.duplicate-ack	TCP packet ACKs data that's already been ACKed.
tcp.segment-outsidewindow	TCP packet is outside the window (TCP module's small window, not real window).
tcp.urgent-nonzero-withouturg- flag	TCP urgent field is non-zero but URG flag isn't set.

Table 12-20 DNS

Term	Description
dns.too-small	DNS packet is too small to contain a valid header.
dns.question-name-past-end	DNS question name goes past the end of the packet.
dns.answer-name-past-end	DNS answer name goes past the end of the packet.
dns.ipv4-address-length-wrong	IPv4 address in DNS response is not 4 bytes long.
dns.answer-circular-reference	DNS answer contains circular reference.

See also[ADM rules syntax on page 124](#)[ADM rule term types on page 127](#)[ADM rule metric references on page 129](#)[Protocol-specific properties on page 131](#)

Advanced Syslog Parser (ASP) rules

The ASP provides a mechanism to parse data out of syslog messages based on user-defined rules.

The Advanced Syslog Parser uses rules to identify where data resides in message-specific events, such as signature IDs, IP addresses, ports, user names, and actions.

When the system receives an ASP log, it compares the time format in the log with the format specified in the ASP rule. If time format doesn't match, the system doesn't process the log.

To increase the likelihood of matching time formats, add multiple custom time formats.

With **Policy Administrator** rights, you can define the order for running ASP rules.

Custom rules

You can write rules to sort parse complex log sources.



This functionality requires knowledge of regular expressions.

The first regular expression determines if a message will be parsed, so write the first rule to look for a pattern that is present in all message you want the rule to parse. Additional regular expressions can be written to capture values from the messages and map them to custom types in the {ESM}. Subsequent regular expressions do not determine the rule match, and are used for parsing only.

While it is possible to test regular expression results on a few log lines in the {Varref: ESM}ESM console itself, we recommend using a graphical tool. There are many free web-based tools that can be used in addition to standalone installable tools. Optionally, another useful tool would be a text editor that supports regular expression searches. Any tools used to test regular expressions need to support pcre expressions.



Ensure regular expressions are written to maximize efficiency. Poorly written expressions can adversely affect parsing performance.

Best practices

Optimize your rules by:

- Thoroughly understand the value that a log can provide to your organization.
- Ensure that captured values align with the intended use of the specific custom type fields.
- Avoid indexing fields that contain unique and random or high cardinality data (such as URLs).
- Ensure that rules mapping event messages directly from the log do not map unique, random, or high cardinality strings as messages. ESM creates a data source rule for each unique event message, and numerous unique strings can reduce ESM performance.
- Categorize events by adding a normalized category to the rule. Data source rules, generated by parsing rules, inherit the normalization assigned to the main parsing rule. If the main parsing rule is left normalized to "Uncategorized," then the parsed events are also normalized as "Uncategorized," making a search for "Uncategorized" events to find unparsed events inaccurate.

See also

[Add a custom ASP rule on page 379](#)

[Set order for ASP and Filter rules on page 382](#)

[Add time formats to ASP rules on page 383](#)

Add a custom ASP rule

The **Advanced Syslog Parser Rule** editor allows you to create rules to parse ASP log data.

Before you begin

User must have administrator rights.

User must have a working knowledge of Perl-Compatible Regular Expressions.

Task

- 1 In the **Policy Editor**, select **Receiver | Advanced Syslog Parser**.
- 2 Click **New**, and then click **Advanced Syslog Parser Rule**.

- 3 Select the General tab and fill in the information.

Table 12-21 Option definitions

Option	Definition
Name	Type a unique, descriptive name for the rule. This text appears in the ESM views when the rule matches a log (unless the message is mapped directly from the log text in the rule).
Tags	Assign tags to the rule. Assign one or more tags to which this rule belongs. This helps in finding and grouping sets of rules created for a given device or application in the policy editor. Any tags added to a rule, causes ESM to automatically include the rule in any policy that has enabled the given tagged rule set.
Default Normalized ID	Many views, correlation rules, and reports use this field as a filter. Select the most relevant value to get the maximize performance.
Default Severity	If the log message does not contain a value for severity, then the event will be assigned the severity value you enter here. Default is 25, valid values are 1-100 (1 is the lowest severity).
Rule Assignment	Rules can be grouped. This pull-down menu provides a list of supported products to group the parsing rules by, separating the events from other data sources. This allows the event to be reported for a specific product.
Description	Type a clear and complete description that conveys the scope and purpose of the rule.

- 4 Select the Parsing tab and fill in the information.

Table 12-22 Option definitions

Option	Definition
Process Name	Similar to the content string filter, but only applies to the process name found within the SYSLOG header. Syslog header formats vary widely, so use content strings when possible.
Content String	<p>If a fixed string is always going to be found in the log, then add it as a content string. The content string(s) of an ASP rule should uniquely identify each log. To speed up rule execution, include at least one content string in each ASP rule. This serves as a pre-filter for optimization - only logs that match the given content strings will be considered for matching and parsing by the regular expressions. The log must contain all defined content strings.</p> <p>Ensure there is at least one value in the content field section. Content strings should be at least three characters long and should be as unique as possible for the specific event. It is advised to include enough content matches to uniquely identify the log. Using one or more content fields in the ASP rule will significantly speed up the matching and parsing process on the Receiver.</p> <p>For example, if the log entry is in this format: <180>Jan 1 00:00:00 testhost ftpd[4325]: FTP LOGIN FROM test.org [192.168.1.1], anonymous, you might add content fields for "ftpd" and "FTP LOGIN FROM".</p>
Regular Expression	The first regular expression determines if the ASP rule will match the log. Any additional expressions will be used to capture values from the log that may or may not be found in all logs.
Named Captures	Use named captures to more easily identify capture groups. The label used for the named capture can consist of alpha-numeric and underscore characters but cannot begin with a number or include a space. The regular expression syntax for a named capture is: (?P<NAME>regular expression capture). For example, a named capture where hostname is the name assigned to the capture group would be: Host\\x3d(?P<hostname>\\S+). When using named captures the policy editor displays the capture name instead of the capture number, in the right-hand side of the Parsing tab as shown below.
Sample Log Data	Paste a sample log entry to be parsed. The parts of the log that match your regular expressions will be highlighted in blue.

Table 12-22 Option definitions *(continued)*

Option	Definition
Format	<p>ASP can pre-process certain logging formats to simplify the mapping of data. The following formats are available:</p> <ul style="list-style-type: none"> • Generic - This is the default and should be used if the log does not match the other available formats. • CEF - (Common Event Format) - This eliminates the need to create a regular expression for each capture, and will allow the data to be mapped using the CEF key names found in the log. • JSON - Similar to CEF, this eliminates the need to create a regular expression for each capture, and will allow data to be mapped using the JSON key names found in the log • XML - Basic, Simple, or Positional - This will allow ASP to parse logs that are in XML format and assign parsed data. The XML format choice will depend upon the type of XML that is within the logs. <ul style="list-style-type: none"> • XML - Basic: expects XML without any repeated elements. • XML - Simple: expects XML with either a single node with attributes, or a single set of non-repeated elements without nesting. • XML - Positional: Expects XML that can have multiple nodes with attributes and multiple repeated elements with nesting.
Parsed Values	<p>The Key/Value fields on the right display what is being parsed from the log sample(s) by the regular expression(s). The Key will display two numbers, separated by a colon. The first number indicates the regular expression being used, and the second number indicates the capture group used within that regular expression. If a captured value is the fourth capture in the third regular expression defined, the key would display 3:4.</p>
Only use regular expressions for parsing purposes	<p>The parser uses the content string (instead of a regular expression) for matching. Regular expressions are used only to parse messages.</p>
Case Insensitive	<p>If the log may contain either upper or lower case letters in some fields, it may be simpler to write the expression in the same case and then use this option. This enables the case insensitivity option for all regular expressions defined in the parsing rule.</p>
Trigger when data doesn't match	<p>Triggers the rule when the regular expression does not match the log.</p>

- 5 Select the Field Assignment tab and fill in the information.
 - a Drag and drop the Values from the right hand side to the Expression column next to the Field on the left.
 - b If the field is not displayed that is needed, click + above the Sample Value column, to display all custom type fields.
 - c Select the desired field and then select OK.

- 6 Select the Mapping tab and fill in the information.

Table 12-23 Option definitions

Option	Definition
Time Format	The date/timestamp of a log message can be parsed using the variables defined in these fields. Many standard date/timestamps are recognized automatically by ESM, however there may be a format that is not recognized or that should be display differently. This section will allow for formatting the time to show up in the proper format when parsed.
Action Mapping	Use this option if there is an action found within the log to be mapped to an available ESM.
Severity Mapping	The severity mapping allows for a value within the log to be mapped to a severity from 1-100. For example, a vendor might define their severity as either Low, Medium, or High in their logs. With the Severity Map section the severity value can map Low as 25, Medium as 50, and High as 75.

- 7 Click **Finish**.
- 8 In the **Policy Editor** window, select the new rule.
- 9 Click **disabled** and then select **enabled**.
- 10 Click the **Rollout** icon in the upper right corner of the window.
- 11 If prompted to save the rule, click **Yes**.
- 12 In the **Rollout** window, click **OK**.

See also

[Advanced Syslog Parser \(ASP\) rules on page 378](#)

[Set order for ASP and Filter rules on page 382](#)

[Add time formats to ASP rules on page 383](#)

Edit ASP Rule Text


If you are an advanced user with knowledge of ASP syntax, add ASP rule text directly so you don't need to define the settings on each tab.

Set order for ASP and Filter rules

If you have **Policy Administrator** rights, you can now set the execution order for Filter or ASP rules. This option sorts your rules efficiently to give you the data that you need most.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM console, click the **Policy Editor** icon .
- 2 On the **Operations** menu, select **Order ASP Rules** or **Order Filter Rules**, then select a data source in the **Data source type** field.

The left pane is populated with the rules that are available to put in order. The ordered rules are in the right pane.
- 3 On the **Standard Rules** or **Custom Rules** tab, move a rule from the left pane to the right pane (drag and drop or use the arrows), placing them above or below **Unordered Rules**.



Unordered Rules represents the rules in the left pane, which are those that are in default order.

- 4 Use the arrows to reorder the rules, then click **OK** to save the changes.

Table 12-24 Option definitions

Option	Definition
Data source type	Select the type of data source this order applies to. The list of rules changes based on the data source selected.
Left table	Select the Standard Rules or Custom Rules tab. Each tab lists the rules that are in default order (alphabetical).
Right table	View the rules that are in a specified order. The Unordered Rules item shows the placement for all rules that are in default order.
Arrows between the tables	Use the right and left arrows to move the selected rules from one table to the other. Use the up and down arrows to place the rules in the table on the right in the correct order.
Revert to default order	Click to return the rules to the default order. When you select this option, all rules in the right table are moved back to the left table.

Table 12-25 Option definitions

Option	Definition
Left table	Select the Standard Rules or Custom Rules tab. Each tab lists the rules that are in default order (alphabetical).
Right table	View the rules that are in a specified order. The Unordered Rules item shows the placement for all rules that are in default order.
Arrows between the tables	Use the right and left arrows to move the selected rules from one table to the other. Use the up and down arrows to place the rules in the right table in the correct order.

See also

[Advanced Syslog Parser \(ASP\) rules on page 378](#)

[Add a custom ASP rule on page 379](#)

[Add time formats to ASP rules on page 383](#)


Add time formats to ASP rules

When the system receives an Advanced Syslog Parser (ASP) log, the time format has to match the format specified in the ASP rule.

You can add multiple custom time formats to increase the likelihood that the time format for the log will match one of the given formats.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM console, click the **Policy Editor** icon .
- 2 In the **Rule Types** pane, click **Receiver | Advanced Syslog Parser**.
- 3 After the ASP rules download, do one of the following:
 - To edit an existing rule, click the rule, then click **Edit | Modify**.
 - To add a new rule, click **New | Advanced Syslog Parser Rule**, then complete the **General**, **Parsing**, and **Field Assignment** tabs.
- 4 Click the **Mapping** tab, then click the plus icon above the **Time Format** table.
- 5 Click in the **Format** field, then select the time format.

6 Select the time fields that you want to use this format.



First Time and **Last Time** refer to the first and last time the event is generated. Any **Custom Type** time fields that you added to the ESM (see *Custom type filters*) are also listed.

7 Click **OK**, then complete the remaining information on the **Mapping** tab.

Table 12-26 Option definitions



Tab	Option	Definition
	File	Click to save the rule, then select Save or Save As .
	Tools	Select Edit ASP Rule Text to add the ASP rule text directly instead of defining the settings on each tab. You must be an advanced user with knowledge of ASP syntax.
General tab		Define general settings for the rule.
	Name	Type a name for the rule.
	Tags	Click Select to add tags that define the categories the rule belongs to. Each ASP rule needs at least one tag for the rule to be saved.
	Default Normalized ID	The default ID is 4026531840, which is uncategorized, and is used if the incoming log doesn't have an ID. To change it, click the icon  and select the ID you want to associate with this rule.
	Default Severity	If needed, change the severity of this rule. This severity gets used if the incoming log data doesn't have a severity.
	Rule Assignment Type	Select a default rule assignment type, which is used to group event data learned from the Advanced Syslog Parser and separate it from other data sources. It is beneficial to group devices with different rule types separately to prevent signature ID collisions in the database. For example, Event 30405 on a Cisco PIX has a different meaning than 30405 on a Cisco IOS or 30405 on a Snort IDS.
	Description	(Optional) Enter a description of the rule.
Parsing tab		Set up the parsing for the rule.
	Process name	(Optional) Type a name for the process which is matched in the header on the incoming log data.
	Content strings	(Optional) Type content strings to be matched on incoming log data. To add a string, click Edit Add , then enter string values, which you must enclose in quotes (") and separated by commas (,).
		 When concatenating a literal value with a PCRE subcapture in ESM 9.0.0 and later, put the literals in quotes individually if they contain spaces or other characters. Leave the PCRE subcapture references unquoted.
	Only use regular expressions for parsing purposes	By default, the rule triggers if the content string or the regular expression match. Select this option if you only want it to trigger if the content string matches.
	Case Insensitive	Select this option if you want content matched regardless of the case.
	Trigger when data doesn't match	Select this option to disable field assignment and mapping. The rule triggers but no data is parsed.

Table 12-26 Option definitions *(continued)*









Tab	Option	Definition
	Regular Expression	<p>Type regular expressions to be used to match against incoming log data, which gives you the ability to do multiple matches on log data. The options are:</p> <ul style="list-style-type: none"> The add icon  launches the Add Regular Expression page where you can enter a regular expression. The edit icon  launches the Edit Regular Expression page so you can make changes to the regular expression selected. The delete icon  deletes the regular expression selected. <div>  <p>These expressions do not execute unless the first one in the list is executed and returns a result from the log data. You can single select regular expression values within this table, which then highlight corresponding text matches within the sample data field with making the selections to the right in the Regular Expression Matches table.</p> </div>
	Regular Expression Matches	This table shows the values that were extracted from the sample log data when run against the primary and secondary regular expressions.
	Include syslog header in regular expression match	Select this option if you want the regular expression matching to be done on the entire log data.
	Sample Log Data	<p>Copy and paste some sample log data into this field to help you create valid regular expressions.</p> <div>  <p>Each log must be on a single line.</p> </div>
	Transformed Log Data	If the original sample log data is in CEF format, it is transformed to the parsing format and shown on this tab. A CEF log that doesn't have custom fields (such as cs1... cs1label... cn1... cn1label...) doesn't need to be transformed.
	Format	Select the format that the Sample Log Data statement is in. If the log data doesn't conform to the standards for the format you select, the key/value pairs are not extracted.
	Key/Value Table	This table shows the key/value pairs extracted from the sample log data.
Field Assignment tab		Set up the field assignments.
	Fields	This column lists the fields that you can match on. You can add fall-back fields by clicking the add icon next to the field name. A fall-back field is used if the primary field is blank. Fall-back fields get executed in order so you can reorder the fields by dragging and dropping them. You can have up to 10 fall-back fields. Once a fall-back field has been added, you can remove it by clicking the delete icon to the left of the fall-back field name.
	Expression	This column is used for mapping fields to log data values. Click the Expression column and type in the group ID in the field that opens. You can concatenate two values by typing the plus (+) sign between them.
	Sample Value	This column is used to simulate what the final output is for a specific field.
	Key/Value Table	This table reflects the values that were extracted from Sample Log Data on the Parsing tab when run against the expressions. You can drag a value from this list and drop it on a field expression.

Table 12-26 Option definitions *(continued)*

Tab	Option	Definition
	Add Custom Field icon and Delete Custom Field icon	If the field you need is not displayed in the Field column, click the Add Custom Field icon  . The Custom Types page lists all custom types on the system, including any you added. Click the field you want to add to the list, then click OK . The field is added to the table. To delete a custom field from the list, click the Delete Custom Field icon  and click Yes to confirm.
Mapping tab		Define custom settings for incoming log data that needs to be mapped or parsed in a unique way.
	Start time and Stop time Custom Format	When the system receives an ASP log, the time format has to match the format specified in the ASP rule. You can add multiple custom time formats. This increases the likelihood that the time format for the log matches one of the given formats (see <i>Add time formats to ASP rules</i>).
	Action table	Click a line in the Action Key column, then enter the different actions that can occur. The Action Value column displays a list of all possible actions. Match the wanted action in the column to the different kinds of actions that can occur.
	Default action	To set a default action to be used if one is not selected in the Action table, click the checkbox and select the action.
	Severity Mapping	You can add values that you want mapped from the incoming log data by clicking the add icon  .
	Default severity	To set a default severity to be used if one is not selected in the Severity Mapping table, select this option, then select the severity.

See also[Advanced Syslog Parser \(ASP\) rules on page 378](#)[Add a custom ASP rule on page 379](#)[Set order for ASP and Filter rules on page 382](#)**Import a log sample**

Use a sample log to test a new rule.

Before you begin

At least one sample log, in plain text format, must be available.

Task

- 1 From the ESM console, select the data source and then click the **Properties** icon.

The Data Source Properties window opens.

- 2 Click **Upload**.

- 3 Navigate to the log sample file and select it.

- 4 Click **Upload**.

A confirmation appears when the file is successfully uploaded.

- 5 Click **Close**.

- 6 Click **Get Events and Flows**.

The Get Events and Flows window opens.

- 7 Select **Events** and then click **Start**.
- 8 Find the events in the dashboard and verify the newly created ASP rule is parsing as expected.

Correlation rules

The fundamental purpose of the correlation engine is to analyze data flowing from ESM, detect interesting patterns within the data flow, generate alerts that represent these patterns, and insert these alerts into the Receiver's alert database. The correlation engine is enabled when a correlation data source is configured.

Within the correlation engine, an interesting pattern results in data interpreted by a correlation rule. A correlation rule is totally separate and distinct from a firewall or standard rule and has an attribute that specifies its behavior. Each receiver gets a set of correlation rules from an ESM (deployed correlation rule set), which is composed of zero or more correlation rules with any user-defined parameter values set. Like firewall and standard rule sets, a base correlation rule set will be included with every ESM (base correlation rule set), and updates to this rule set are deployed to ESM devices from the rule update server.



The rules on the rule update server include default values. When you update the base correlation engine rule set, you must customize these default values so they properly represent your network. If you deploy these rules without changing the default values, they can generate false positives or false negatives.

Only one correlation data source can be configured per Receiver, in a fashion similar to configuring syslog or OPSEC. Once the correlation data source is configured, you can edit the base correlation rule set to create the deployed correlation rule set using the **Correlation Rule Editor**. You are allowed to enable or disable each correlation rule and set the value of each rule's user definable parameters.

In addition to enabling or disabling the correlation rules, the **Correlation Rule Editor** allows you to create custom rules and create custom correlation components that can be added to correlation rules.

See also

[View correlation rule details on page 389](#)

[Set up correlation rule to compare two fields in an event on page 391](#)

[Override Group by on page 392](#)

Example of custom correlation rule or component

Add a correlation rule or component.

The rule we are going to add in this example generates an alert when the ESM detects five unsuccessful login attempts from a single source on a Windows system, followed by a successful login, all within 10 minutes.

- 1 In the **Rule Types** pane of the **Policy Editor**, click **Correlation**.
- 2 Click **New**, then select **Correlation Rule**.
- 3 Type a descriptive name, then select the severity setting.



Because an event generated by this rule could indicate that an unauthorized person has accessed the system, an appropriate severity setting is 80.

- 4 Select the normalization ID, which could be **Authentication** or **Authentication | Login**, then drag-and-drop the **AND** logic element.



Select **AND** because there are two types of actions that need to occur (login attempts first, then a successful login).




- 5 Click the **Menu** icon  , then select **Edit**.

- 6 Select **Sequence** to indicate that the actions (first, five unsuccessful login attempts and second, a successful login) must occur sequentially, then set the number of times this sequence must occur, which is "1."
- 7 Set the period of time the actions need to occur in, then click **OK**.



Since there are two actions that require time windows, the 10-minute period must be divided between the two. For this example, five minutes is the period of time for each action. Once the unsuccessful attempts have occurred within five minutes, the system begins to listen for a successful login from the same IP source within the next five minutes.

- 8 In the **Group by** field, click the icon, move the **Source IP** option from the left to the right, indicating that all actions must come from the same source IP, then click **OK**.
- 9 Define the logic for this rule or component.

To do this...	Do this...
Specify the type of filter that identifies the events of interest (in this case, multiple failed login attempts against a Windows system).	<ol style="list-style-type: none"> 1 Drag-and-drop the Filter icon  and drop it on the AND logic element. 2 On the Filter Fields Component page, click Add. 3 Select Normalization Rule In, then select: <ul style="list-style-type: none"> • Normalization • Authentication • Login • Host Login • Multiple failed login attempts against a Windows host 4 Click OK.
Set the number of times the login failure needs to occur and the period of time in which they must occur.	<ol style="list-style-type: none"> 1 Drag-and-drop the AND logic element to the Filter bar. <div data-bbox="646 751 1518 835">  The AND element is used because there are five separate attempts that must occur. The element allows you to set the number of times and the length of time that they must occur. </div> 2 Click the Menu icon  for the AND element you just added, then click Edit. 3 In the Threshold field, enter 5 and remove other values that are present. 4 Set the Time Window field to 5. 5 Click OK.
Define the second filter type that needs to occur, which is the successful login.	<ol style="list-style-type: none"> 1 Drag-and-drop the Filter icon to the bottom prong of the first AND logic element's bracket. 2 On the Match Component page, click Add. 3 In the fields, select Normalization Rule In, then select: <ul style="list-style-type: none"> • Normalization • Authentication • Login • Host Login 4 Click OK to return to the Match Component page. 5 To define "successful," click Add, select Event Subtype In, then click the Variables icon and click Event Subtype success Add. 6 Click OK to return to the Policy Editor.

The new rule is added to the list of correlation rules on the **Policy Editor**.

View correlation rule details


Correlation rules display details about what caused the rule to trigger. This information can help you tune for false positives.

Before you begin

Verify that you have administrator rights or belong to an access group with policy administration permission.

Details are always gathered at the time of request. But for rules that use dynamic watchlists or other values that might change often, set the rule to get details immediately after triggering. This reduces the chance that details are unavailable.

Task

- 1 From the dashboard, click  and select **Correlation**.
The Policy Editor displays a list of your correlation rules.
- 2 Set each rule to show the details immediately.
 - a On the ESM console, click the **Policy editor** icon, then click **Correlation** in the **Rule Types** pane.
 - b Click the **Details** column for the rule and select **On**.
You can select more than one rule at a time.
- 3 View the details:
 - a On the system navigation tree, click **Rule Correlation** under the ACE device.
 - b From the view list, select **Event Views | Event Analysis**, then click the event you want to view.
 - c Click the **Correlation Details** tab to view the details.

See also

[Correlation rules on page 387](#)

[Set up correlation rule to compare two fields in an event on page 391](#)

[Override Group by on page 392](#)

Add parameters to a correlation rule or component

The parameters of a correlation rule or component control the behavior of the rule or component when it executes. Parameters are not required.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the **Correlation Rule** or **Correlation Component** pages, click **Parameters**.
- 2 Click **Add**, then enter a name for the parameter.
- 3 Select the type of parameter you want this to be, then select or deselect the values.



List and Range values can't be used at the same time. A list value cannot include a range (1–6, 8, 10, 13). The correct way to write it is 1, 2, 3, 4, 5, 6, 8, 10, 13.


- 4 To select the default value for the parameter, click the **Default Value Editor** icon .
- 5 If you do not want the parameter to be externally visible, deselect **Externally Visible**. The parameter is local to the scope of the rule.
- 6 Type a description of this parameter, which appears in the **Description** text box on the **Rule Parameter** page when the parameter is highlighted.
- 7 Click **OK**, then click **Close**.

Table 12-27 Option definitions

Option	Definition
Name	Type a name for the parameter.
Type	Select the type of parameter this is.
Values that can be	Select or deselect the values to be entered into this parameter. List and Range values cannot be used at the same time. A list value cannot include a range (1-6 8, 10, 13). The correct way to write it would be 1, 2, 3, 4, 5, 6, 8, 10, 13.
Default Value	Click the Default Value Editor icon to select the default value for the parameter.
Externally Visible	If you do not want the parameter to be externally visible, deselect this option. The parameter is then local to the scope of the rule.
Description	Type a description of this parameter, which appears in the Description field on the Rule Parameters page when the parameter is clicked.

Table 12-28 Option definitions

Option	Definition
Table	Lists the parameters for the rule with their current value and default value.
Edit	Click to make changes to the value.
Description	Describes the parameter selected on the table.
Restore Defaults	Click to restore the values to their default setting.

Table 12-29 Option definitions

Option	Definition
Table	View existing parameters. If it is a new rule or component, none will be listed.
Add	Add a new parameter for the rule or component.
Edit	Make changes to the settings of an existing parameter.
Delete	Delete a parameter.
Description	View a description of the selected parameter.

Table 12-30 Option definitions

Option	Definition
Table	Select the rule or component that you want to reference.
Description	Displays a description of the selected rule or component.

Set up correlation rule to compare two fields in an event




Using the **Default Value Editor**, you can set up a correlation rule to compare the values in two different fields in an event.

For example, you can set up a rule to ensure that the source user and destination user are the same. You can also set up one that ensures that the source IP address and destination IP address are not the same.

For numeric fields, greater than (>), less than (<), greater than or equal to (>=), and less than or equal to (<=) operators are supported.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the ESM console, click the **Policy Editor** icon .
- 2 In the **Rule Types** pane, select **Correlation**, click the rule you want to compare fields in, then click **Edit** | **Modify**.
- 3 Click the menu icon of a logic component , then click **Edit**.
- 4 In the filters area, click **Add** and add a new filter, or select an existing filter and click **Edit**.
- 5 Click the **Default Value Editor** icon , type the value and click **Add**, then select the field on the **Fields** tab and click **Add**.

See also

[Correlation rules on page 387](#)

[View correlation rule details on page 389](#)

[Override Group by on page 392](#)




Override Group by

If you have set a correlation rule to group by a specific field, you can override one of the components in the rule to match on a different field.

For example, if you set the **Group by** field in a correlation rule to **Source IP**, you can override a component of the rule to use **Destination IP**. This means that all events have the same source IP except the events that match the overridden component. Those events have the same destination IP as the source IP of the other events. This feature is useful to look for one event going to a particular destination followed by another event that originates from that destination.

Task

For details about product features, usage, and best practices, click [?](#) or [Help](#).

- 1 On the ESM console, click the **Policy Editor** icon .
- 2 Click **Correlation** in the **Rule Types** pane, select a rule, then click **Edit** | **Modify**.
- 3 Drag and drop the **Match Component** logic element  in the **Correlation logic** area, then click the menu icon , or click the menu icon of an existing **Match Component** element in the **Correlation logic** area.
- 4 Select **edit**, click **Advanced Options**, then select **Override Group By** and click **Configure**.
- 5 On the **Configure Group By overrides** page, select the override field, then click **OK**.

See also

[Correlation rules on page 387](#)

[View correlation rule details on page 389](#)

[Set up correlation rule to compare two fields in an event on page 391](#)

Data source rules

The list of data source rules includes predefined and auto learned rules.

The Receiver auto learns data source rules as it processes the information sent to it by the data sources that are associated with the Receiver.

The **Data Source** option in the **Rule Types** pane is only visible when a policy, data source, **Advanced Syslog Parser**, or Receiver is selected in the system navigation tree. The description area at the bottom of the page gives detailed information concerning the selected rule. All rules have a severity setting that dictates the priority associated with a rule. The priority impacts how the alerts generated for these rules are shown for reporting purposes.

Data source rules have a defined default action. The Receiver assigns it to the event subtype associated with the rule. You can change this action (see *Set data source rule actions*).

See also

[Set data source rule actions on page 393](#)

[Manage auto-learned data source rules on page 393](#)

Add or edit a data access rule

DEM data access policies provide the ability to track unknown access paths into the database and to send events in real-time.

Common violations in database environments, such as application developers accessing production systems using application logon IDs, can be easily tracked when create the appropriate data access policies.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane on the **Policy Editor**, select **DEM | Data Access**.
- 2 Do one of the following:
 - To add a new rule, select **New**, then click **Data Access Rule**
 - To edit a rule, select the rule in the rules display pane, then click **Edit | Modify**.
- 3 Fill in the information, then click **OK**.


Set data source rule actions

Data source rules have a defined default action. The Receiver assigns this action to the event subtype associated with the rule. You can change this action.

You can set the value of the event subtype per data source rule. This means that you can set rule actions for dashboards, reports, parsing rules, or alarms with different values, such as the outcome of a selective access rule (permit/deny).

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the ESM console, click the **Policy Editor** icon , then select **Receiver | Data Source** in the **Rule Types** pane.
- 2 Click in the **Subtype** column for the rule you want to change, then select the new action.
 - Select **enable** to populate the event subtype with the default action, **alert**.
 - Select **disable**, if you don't want to collect events for the corresponding rule.
 - Select any other action to populate the event subtype with that action.

See also

[Data source rules on page 392](#)


[Manage auto-learned data source rules on page 393](#)

Manage auto-learned data source rules

View a list of all auto-learned data source rules and edit or delete them.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the **Policy Editor**, select **Receiver | Data Source**.
- 2 On the **Filters/Tagging** pane, click the **Advanced** bar at the bottom of the pane.
- 3 On the **Origin** drop-down list, select **user defined**, then click the **Run Query** icon .

All the auto-learned data source rules are listed in the display pane.

- 4 Select the rule you want to edit or delete, click **Edit**, then select **Modify** or **Delete Auto Learned Rules**.
 - If you selected **Modify**, change the name, description, or normalized ID, then click **OK**.
 - If you selected **Delete Auto Learned Rules**, select the correct option, then click **OK**.

Table 12-31 Option definitions

Option	Definition
Delete all auto learned rules for this data source type	Deletes all the rules that have been auto learned for the selected data source.
Delete selected auto learned rules	Deletes the rules you selected on the rules display pane.
Delete all auto learned rules previous to this time	Deletes the rules that were auto learned prior to the date you enter in the field.
Delete all auto learned rules previous to the system retention time	Deletes the rules that were auto learned prior to the date you have set as the system retention time. If you need to change the data retention time, click Edit .

See also

[Data source rules on page 392](#)

[Set data source rule actions on page 393](#)

DEM rules

The true power of McAfee DEM lies in the way it captures and normalizes the information in network packets.

DEM also has the ability to create complex rules using logical and regular expressions for pattern matching, which provides the ability to monitor database or application messages with virtually no false positives. The normalized data (metrics) vary for each application because some application protocols and messages are richer than others. Filter expressions must be carefully crafted, not only the syntax but also by making sure that the metric is supported for the application.

The DEM ships with a default set of rules. Default compliance rules monitor significant database events such as logon/logoff, DBA-type activity such as DDL changes, suspicious activity, and database attacks that are typically required to achieve compliance requirements. You can enable or disable each default rule and set the value of each rule's user-definable parameters.

These are the types of DEM rules: Database, data access, discovery, and transaction tracking.

Rule types	Description
Database	<p>The DEM default rule set includes rules for each supported database type and common regulations like SOX, PCI, HIPAA, and FISMA. You can enable or disable each of the default rules and set the value of each rule's user-definable parameters.</p> <p>In addition to using the rules that are shipped with the DEM, you can create complex rules using logical and regular expressions. This provides the ability to monitor database or application messages with virtually no false positives. Because some application protocols and messages are richer than others, the normalized data (metrics) vary for each application.</p> <p>Rules can be as complex as you require and include both Logical and Regular Expression operators. A Rule Expression can be applied against one or more metrics available for the application.</p>
Data access	<p>The DEM's data access rules provide the ability to track unknown access paths into the database and send alerts in real time. Common violations in database environments, such as application developers accessing production systems using application logon IDs, can be easily tracked once you create the appropriate data access rules.</p>
Discovery	<p>The DEM's database discovery rules provides an exception list of database servers, of the types supported by the ESM, that are on the network but are not being monitored. This allows a security administrator to discover new database servers being added to the environment and illegal listener ports opened to access data from databases. The discovery rules (Policy Editor DEM Rule Type Discovery) are out-of-box rules that can't be added to or edited. When the discovery option on the database servers page is enabled (DEM Properties Database Servers Enable), the system uses these rules to search for database servers that are on the network, but are not listed under the DEM on the system navigation tree.</p>
Transaction tracking	<p>Transaction tracking rules allow you to track database transactions and auto-reconcile changes. For example, the time-consuming process of tracking database changes and reconciling them with authorized work orders in your existing change ticketing system can be fully automated.</p> <p>Use of this feature is best understood with an example:</p> <p>The DBA, as a matter of procedure, would execute the start tag stored procedure (spChangeControlStart in this example) in the database where the work would be performed before actually beginning the authorized work. The Transaction Tracking feature in the DEM allows the DBA to include up to three optional string parameters as argument to the tag in the correct sequence:</p> <ol style="list-style-type: none"> 1 ID 2 Name or DBA Initials 3 Comment <p>For example, <code>spChangeControlStart '12345', 'mshakir', 'reindexing app'</code></p> <p>When the DEM observes the spChangeControlStart procedure being executed, it not only logs the transaction but also the parameters (ID, Name, Comment) as special information.</p> <p>Once the work is complete, the DBA executes the end tag stored procedure (spChangeControlEnd) and optionally includes one ID parameter, which must be the same as the ID in the begin tag. When the DEM observes the end tag (and ID) it can associate all activity between the start tag (which has the same ID) and end tag as a special transaction. You can now report by transactions and search by ID, which in this work order reconciliation example could be the change control number.</p> <p>You can also use transaction tracking to log start and end of a trade execution or even begin and commit statements to report by transactions instead of queries.</p>

ESM rules

ESM rules are used to generate events that are related to the ESM.

All the rules of this type are defined by McAfee. They can be used to generate compliance or auditing reports that show what has occurred on the ESM. You cannot add, modify, or delete them. You can, however, change the property settings (see *Rule types and their properties*).

Filter rules

Filter rules allow you to specify the action to take when data that you define is received by the Receiver.

Data order

Filter rules are written to the Receiver in this data order:

- 1 All non "catch-all" rules.
 - a stop = true and parse = false and log = false
 - b stop = true and parse = true and log = true
 - c stop = true and parse = true and log = false
 - d stop = true and parse = false and log = true
- 2 All "catch-all" rules

Rule order

If you have **Policy Administrator** rights, you can define the order that you want the Filter rules to run in. These rules then run in the most effective order to generate the data you need (see *Set order for ASP and Filter rules*).

Add Filter rules

You can add Filter rules to the **Policy Editor**.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the **Policy Editor**, select **Receiver | Filter**.
- 2 Select **New**, then click **Filter Rule**.
- 3 Complete the fields, then click **OK**.
- 4 To enable the rule, select the rule in the rule display pane, click the setting in the **Action** column, then click **enabled**.

Table 12-32 Option definitions

Option	Definition
Tags	<ul style="list-style-type: none"> Click Select and choose tags to define the categories this rule belongs to.
Name	<ul style="list-style-type: none"> Type a name for the rule.
Normalized ID	<ul style="list-style-type: none"> (Optional) Click the Normalized ID icon, then select any additional normalized IDs.
Severity	<ul style="list-style-type: none"> (Optional) Change the severity setting for the rule.
Match All	<ul style="list-style-type: none"> Select if you want the rule to be written without PCRE or content strings. If you select this option, the actions you specify in the Action to take with this rule section will be performed on all the data that is received.
Content Strings	(Optional) Type content strings to filter the data that is being received. When the data received matches these content strings, the action you specify on this dialog will be performed. <ul style="list-style-type: none"> To add a string, click Add and enter the string. To edit or remove a string, select the string and click the corresponding button.

Table 12-32 Option definitions *(continued)*

Option	Definition
PCRE	• (Optional) Type a single PCRE to filter the data that is being received. When the data received matches this PCRE, the action you specify on this dialog will be performed.
Case Insensitive	• Select if you want to add a case insensitive modifier so the PCRE content is matched regardless of the case.
Action	Select the actions that will be taken when the data received matches the PCRE and content strings, or on all the data received if Match All is selected. You can select as many of these actions as needed.
Description	• (Optional) Type a description for the rule. It will appear in the Description field of the Policy Editor when the rule is selected.

Table 12-33 Option definitions

Option	Definition
Filter types	Select what it will filter on.
Filter conditions	Select the filter condition. The options available vary based on the type you selected.
Values	Click the variables icon, then select the values for this filter.

Add or edit a transaction tracking rule

Transaction tracking rules track database transactions and auto-reconcile changes, as well as log start and end of a trade execution or begin and commit statements to report by transactions instead of queries.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the **Policy Editor**, select **DEM | Transaction Tracking**.
- 2 Do one of the following:
 - To add a new rule, click **New**, then click **Transaction Tracking Rule**.
 - To edit a rule, select the rule on the rules display pane, then click **Edit | Modify**.
- 3 Fill in the information, then click **OK**.

Table 12-34 Option definitions


Option	Definition
Type	Select the type of transaction tracking rule this is.
Rule Name	Type a name for the rule. It must be unique; should be descriptive; and can only contain alphanumeric characters, underscores (_), and spaces.
Start Query Tag	Type the SQL query to be executed prior to making changes to the database (for example, spChangeControlStart).
Stop Query Tag	Type the SQL query to be executed after making changes to the database (for example, spChangeControlEnd).
Tags	Click Select , select tags you want to associate with this rule, then click OK .
Normalized ID	To change the default, click the icon  , then select the ID.

Table 12-34 Option definitions *(continued)*

Option	Definition
Severity	Select the severity setting.
Description	Type a description of the rule.

Variables

A *variable* is a global setting or a placeholder for information that is user- or site-specific. Many rules use variables.



We recommend that you have extensive knowledge of Snort format before adding or modifying variables.

Variables are used to make rules behave in a specific way, which might vary from device to device. The ESM has many pre-set variables, but also provides the ability to add custom variables. When adding a rule, these variables appear as options in the drop-down list for the field type selected in the **Type** field on the **New Variable** page.

Each variable has a default value, but we recommend that you set some values that correspond to the specific environment of each device. No spaces are allowed when entering a variable name. If a space is necessary, use the underscore (`_`) character. To maximize the effectiveness of a device, it is particularly important to set the HOME_NET variable to the home network being protected by the specific device.

This table shows a list of common variables and their default values.

Variable names	Description	Default	Default description
EXTERNAL_NET	Everyone outside of the protected network	!\$HOME_NET	Port 80
HOME_NET	Local protected network address space: (10.0.0.0/80)	Any	Same as HOME_NET
HTTP_PORTS	Web server ports: 80 or 80:90 for a range between 80 and 90	80	Any port except the HTTP_PORTS
HTTP_SERVERS	Addresses of web servers: 192.168.15.4 or [192.168.15.4,172.16.61.5]	\$HOME_NET	Same as HOME_NET
SHELLCODE_PORTS	Anything but web server ports	!\$HTTP_PORTS	Same as HOME_NET
SMTP	Mail server addresses	\$HOME_NET	Same as HOME_NET
SMTP_SERVERS	Mail server addresses	\$HOME_NET	Same as HOME_NET
SQL_SERVERS	Addresses of SQL DB servers	\$HOME_NET	Same as HOME_NET
TELNET_SERVERS	Addresses of telnet servers	\$HOME_NET	Same as HOME_NET

Variables that come with the system can be modified. Custom variables can be added, modified, or deleted.

You can assign types to custom variables. Variable types are used when filtering rules for reporting and they determine the field in which the variables are available when adding or modifying a rule. Variable types are global in nature, and any changes that are made are reflected on all levels of the policy.

See also

[Manage variables on page 398](#)

[Detect TCP protocol anomalies and session hijacking on page 400](#)

Manage variables

When you select the variable rule type on the **Policy Editor**, you can take several actions to manage both custom and predefined variables.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 Click the **Policy Editor** icon.
- 2 On the **Rule Types** pane, select **Variable**.
- 3 Do any of the following:



To...	Do this...
Add a new category	<ol style="list-style-type: none"> 1 Select New Category. 2 Enter a name for the new category, then click OK.
Add a custom variable	<ol style="list-style-type: none"> 1 In the rules display pane, select the category, then click New. 2 Select Variable, then define the requested settings. 3 Click OK.
Modify a variable	<ol style="list-style-type: none"> 1 In the rules display pane, select the variable to be modified. 2 Select Edit, then click Modify. 3 Modify the value or description, then click OK.
Delete a custom variable	<ol style="list-style-type: none"> 1 In the rules display pane, select the variable to be removed. 2 Select Edit, then click Delete.
Import a variable	<ol style="list-style-type: none"> 1 Select File, then click Import Variables. 2 Click Import, then browse and upload the file. <div>  The import file must be a .txt file containing the following information in this format: VariableName;VariableValue; CategoryName (optional); Description (optional). If one field is missing, a semi-colon must be in place to act as a place holder. </div>
Modify the type of custom variable	<ol style="list-style-type: none"> 1 Select the custom variable. 2 Click Edit, then select Modify. 3 Change the variable type. <div>  When the variable type is set to something other than No Type Selected and committed, you can't change the value. </div> <ol style="list-style-type: none"> 4 Click OK to save changes.

Table 12-35 Option definitions

Option	Definition
Name	Type a name for the new variable.
Type	Select the type of variable this will be. Once you add the variable, this setting can't be changed.
Value	Type the value for the type of variable this is.
Description	(Optional) Type a description of the variable.

Table 12-36 Option definitions

Option	Definition
Name	The name of this variable. It can't be modified.
Type	The type of variable this is. It can't be modified.
Value	The value for this variable. You can change it to any of the values described in the Description field.
Description	A description of the variable and its options.

Table 12-37 Option definitions

Option	Definition
Import	Browse to the file of variables that you want to import to the Policy Editor .

See also


[Variables on page 398](#)

Detect TCP protocol anomalies and session hijacking

You can detect and alert on TCP protocol anomalies and check to TCP session hijacking using the Stream5 preprocessor variable.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the ESM console, click the **Policy Editor** icon .
- 2 In the **Rule Types** pane, click **Variable**.
- 3 In the rules display pane, click **preprocessor**, then select **STREAM5_TCP_PARAMS**.
- 4 On the **Modify Variable** page, add one of the following in the **Value** field:
 - To detect and alert on TCP protocol anomalies, add `detect_anomalies` after **policy first**.
 - To check for TCP session hijacking, add `detect_anomalies check_session_hijacking` after **policy first**.

See also

[Variables on page 398](#)

Windows events rules

Windows events rules are used to generate events that are Windows related.

They are data source rules for Windows events and are separated from the data source rule type because they are a common use case. All rules of this type are defined by McAfee. You can't add, modify, or delete them, but you can change their property settings.

Default Policy settings


You can set up the default policy to operate in alerts only mode or oversubscription mode. You can also view the status of the rule updates and initiate an update.

Set up Oversubscription Mode

Oversubscription Mode defines how packets are handled if the device's capacity is exceeded. In each case, the packet is recorded as an event.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the **Policy Editor**, click the **Settings** icon .
- 2 In the **Oversubscription Mode** field, click **Update**.
- 3 In the **Value** field, enter the functionality.
 - a Pass (pass or 1) allows packets that would be discarded to pass unscanned.
 - b Drop (drop or 0) drops packets that exceed the device's capacity.
 - c To pass or drop a packet without generating an event, enter `spass` or `sdrop`.
- 4 Click **OK**.



As of version 8.1.0, changing **Oversubscription Mode** affects the device and its children (virtual devices). For this change to take effect, you must change the mode on the parent device.


View policy update status for devices

View a summary of the status of policy updates for all devices on the ESM.

This helps determine when you must roll out updates to your system.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the **Policy Editor**, click the **Settings** icon .
- 2 In the **Status** field, view the number of devices that are up to date, out of date, and scheduled for an auto rollout.
- 3 Click **Close**.

Rule operations


There are several operations you can perform on the rules to manage them and generate the information needed.

Manage rules

ADM, DEM, Deep Packet Inspection, Advanced Syslog Parser, and Correlation rules can be viewed, copied, and pasted. Custom rules of these types can be modified or deleted. Standard rules can be modified, but must be saved as a new custom rule.

Task

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule that you want to work with.
- 2 Do any of the following:

To do this...	Do this...
View custom rules	<ol style="list-style-type: none"> 1 Select the Filter tab in the Filters/Tagging pane. 2 At the bottom of the pane, click the Advanced bar. 3 In the Origin field, select user defined, then click Run Query .
Copy and paste a rule	<ol style="list-style-type: none"> 1 Select a predefined or custom rule. 2 Select Edit Copy, then select Edit Paste. The rule you copied is added to the list of existing rules, with the same name and settings. <div data-bbox="548 1052 587 1094" data-label="Image"></div> <div data-bbox="609 1058 1373 1089" data-label="Text"> <p>For ASP and Filter Rules, the rule order is copied as part of the copy process.</p> </div> 3 Check that the ordering of the new rule will not adversely affect data parsing (Operations Order ASP Rules) or (Operations Order Filter Rules). 4 To change the name, select Edit Modify.
Modify a rule	<ol style="list-style-type: none"> 1 Highlight the rule you want to view, then select Edit Modify. 2 Change the settings, then click OK. If it's a custom rule, it's saved with the changes. If it is a standard rule, you are prompted to save the changes as a new custom rule. Click Yes. <div data-bbox="522 1404 561 1446" data-label="Image"></div> <div data-bbox="591 1398 1481 1453" data-label="Text"> <p>If you did not change the name of the rule, it is saved with the same name and a different sigID. You can change the name by selecting the rule, then selecting Edit Modify.</p> </div>
Delete a custom rule	<ul style="list-style-type: none"> • Select the custom rule. • Select Edit Delete.

Import rules

You can import a set of rules that has been exported from another ESM and save it to your ESM.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, click the type of policy or rules you are importing.
- 2 Click **File | Import**, then select **Rules**.



These changes are not tracked so they can't be undone.

- 3 Click **Import Rules**, then browse to the file you want to import and select **Upload**.

The file is uploaded to the ESM.

- 4 On the **Import Rules** page, select the action to take if rules being imported have the same ID as existing rules.
- 5 Click **OK** to import the rules, resolving the conflicts as indicated.

The contents of the file are reviewed and the appropriate options are enabled or disabled, depending on the contents of the selected file.

Table 12-38 Option definitions

Option	Definition
Import Rules	Click to select the rules file and upload it to the ESM.
Overwrite existing rules	If there is a conflict when importing, select this if you want to delete the existing rule and overwrite it with the rule that is part of the policy being imported.
Create a new rule when a conflict exists	If there is a conflict when importing, select this if you want to keep both of the rules, creating a new ID for the imported rule.
Skip the rule when an existing rule exists	If there is a conflict when importing, select this if you want to keep the existing rule and not import the conflicting rule.

See also

[Conflicts when importing correlation rules on page 403](#)

Conflicts when importing correlation rules

When you export correlation rules, a file is created that contains the rule data. It doesn't, however, include referenced items such as variables, zones, watchlists, custom types, and assets, which this rule might use.

When the export file is imported to another ESM, any referenced items contained in the rule that do not exist on the importing system results in a rule conflict. For example, if rule one references variable \$abc, and no variable is defined on the importing system that is named \$abc, this condition is a conflict. Conflicts are logged and the rule is flagged as in conflict.

Conflicts are resolved by creating the needed referenced items (manually or through import where applicable) or editing the correlation rule and changing the references within the rule.

If there are rules in conflict, a page is displayed immediately after the import process indicating which rules are in conflict or which failed. Rules can be edited to resolve conflicts from that page, or the page can be closed. Rules in conflict are flagged with an exclamation mark icon indicating their status. Editing a conflicted rule in the rule editor presents a conflicts button, which when clicked, displays the conflict detail for that rule.

See also

[Import rules on page 402](#)

Import variables

You can import a file of variables and change their type. If there are conflicts, the new variable is automatically renamed.

Before you begin

Set up the file to be imported.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, click **Variable**.
- 2 Click **File | Import | Variables**, then browse to the file of variables and click **Upload**.

If there are conflicts or errors in the file, the **Import - Error Log** page opens informing you of each issue.


- 3 On the **Import Variable(s)** page, click **Edit** to change the **Type** for the selected variables.
- 4 Click **OK**.

Export rules

Export custom rules or all the rules in a policy and then import them to another ESM.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, click the type of rules you are exporting.
- 2 Access a list of the custom rules of the type you selected:
 - a In the **Filter/Tagging** pane, make sure the **Filter** tab is selected.
 - b Click the **Advanced** bar at the bottom of the pane.
 - c On the **Origin** drop-down list, select **user defined**.
 - d Click the **Run Query** icon .
- 3 Select the rules you want to export, then click **File | Export | Rules**.
- 4 On the **Export Rules** page, select the format to use when exporting the rules.
- 5 On the **Download** page, click **Yes**, select the location, then click **Save**.



If you open the csv file using Microsoft Excel, some of the UTF-8 characters might be corrupted. To correct this, open the **Text Import Wizard** in Excel and select **Delimited** and **Comma**.








Filter existing rules

When you select a rule type in the **Policy Editor**, all the rules of the selected type are listed in alphabetical order, by default. You can list them by time or use tags to filter the rules so you can view only those that meet your criteria.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule you want to filter.
- 2 Make sure that the **Filter** tab is selected in the **Filters/Tagging** pane.
- 3 Do any of the following:

To...	Do this...
Filter with multiple tags	<ul style="list-style-type: none"> Select categories or tags, then click the Run Query icon . <p>Only those rules that meet all filters are displayed.</p>
View rules that meet either of the filters you select	<ol style="list-style-type: none"> 1 Select more than one category or tag. 2 Click the or icon, then click the Run Query icon. <div>  Fields that are affected by inheritance (Action, Severity, Blacklist, Aggregation, and Copy Packet) cannot be filtered using the or icon. </div>
Search for a specific tag	<ol style="list-style-type: none"> 1 Type the tag's name in the Type here to search for a tag field. 2 Select the one you need from the list of options.
List the rules by the time they were created	<ul style="list-style-type: none"> Click the Sort on Time icon  on the toolbar, then click the Run Query icon.
List the rules in alphabetical order	<ul style="list-style-type: none"> Click the Sort on Name icon  on the toolbar, then click the Run Query icon.
Clear the filtering	<ul style="list-style-type: none"> Click the orange filter icon on the rules display pane title bar . <p>The filters are cleared and all the rules are once again displayed in the rule display pane.</p>
Clear the filter tags	<ul style="list-style-type: none"> Click the Clear All icon  on the toolbar. <p>The tags are cleared but the list of rules remains filtered.</p>
Filter by signature ID	<ol style="list-style-type: none"> 1 Click the Advanced bar at the bottom of the Filter pane. 2 Type the signature ID, then click the Run Query icon.
Filter by name or description	<ol style="list-style-type: none"> 1 In the Advanced pane, enter the name or description. 2 For the results, regardless of case, click the case-insensitive icon Aa.
Filter by device type, normalized ID, or action	<ol style="list-style-type: none"> 1 In the Advanced pane, click the Filter icon . 2 On the Filter Variables page, select the variable.
Compare the differences in the policy-based settings for a rule type and its immediate parent	<ul style="list-style-type: none"> In the Advanced pane, select View Exceptions, then click the Run Query icon.
Filter by severity, blacklist, aggregation, copy packet, origin, and rule status	<ul style="list-style-type: none"> Select the filter from the drop-down list in each of these fields.

To...	Do this...
View only custom rules	<ul style="list-style-type: none"> Select user-defined in the Origin field in the Advanced pane, then click the Run Query icon.
View rules created in a specific time period	<ol style="list-style-type: none"> Click the calendar icon next to the Time field on the Advanced pane. On the Custom Time page, select the start and stop time, click OK, then click the Run Query icon.

View a rule's signature

If you access the McAfee online signature database, you can view information about the signature for a rule. This option is available for firewall, deep packet inspection, and data source rules.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule you want to view.
- 2 Select a rule in the rule display pane.
- 3 Click **Operations**, then select **Browse Reference**.

The **NTAC Vulnerability Summary** screen opens in your browser.

- 4 To view the summary of a signature, click on the links in the **Signatures** section of the screen.

Retrieve rule updates




The McAfee Signature Team continuously updates the rule signatures used by a device to examine network traffic and are available for download from the central server. These rule updates can be retrieved automatically or manually.

Task




See *Override action on downloaded rules* to set up overrides for the actions taken when rules are retrieved from the server.

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the **Policy Editor**, click the **Settings** icon .
- 2 On the **Rules Update** line, click **Update**.
- 3 Set the ESM to retrieve the updates automatically or check for updates now.
- 4 If updates were downloaded manually, click the **Rollout** icon  to apply them.
- 5 To view the manual updates, do the following:
 - a In the **Filters/Tagging** pane, click the **Advanced** bar.
 - b In the **Rule Status** field, selected **Updated**, **New**, or **Update/New** to indicate the type of updated rules you want to view.
 - c Click the **Run Query** icon .

The updated rules are listed with a starburst icon  if they are added or an exclamation point  if they are changed.

Table 12-39 Option definitions

Option	Definition
Auto check every	Select if you want to set the ESM to retrieve the updates automatically. If this is the first time you are updating the rules, the Customer Validation page will open. Enter your customer ID and password, then select Validate .  If you don't remember this information, contact McAfee Support.
hours, minutes	Select the frequency with which you want the system to check for updates.
Check Now	Check for rule updates and download them now.
Manual Update	Click if you want to select the update file to upload.
Credentials	Click to add the credentials given to you by McAfee.


Clear updated rule status

When rules are modified or added to the system. You can clear these markings once you have had the opportunity to review the updates.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule you want to clear.
- 2 Do one of the following:

To...	Do this...
Clear all the rule status markings	<ol style="list-style-type: none">1 Click Operations, then select Clear Updated Rule Status.2 Click All.
Clear selected rules	<ol style="list-style-type: none">1 In the Filters/Tagging pane, click the Advanced bar.2 In the Rule Status field, select Updated, New, or Updated/New to indicate the type of marking you want to clear.3 Click the Run Query icon . <p>The rules with the selected markings are listed in the rule display pane.</p> <ol style="list-style-type: none">4 Select the rules to be cleared.5 Click Operation Clear Updated Rule Status Selected.


Compare rule files

You can compare the policy state (applied, current, rollback, or staged) of Receiver, ADM, and DEM rule files.

This is helpful if you need to see the changes if you apply the current policy to a device. In that case, you would compare the current rules and the applied rules.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, click a Receiver, ADM, or DEM device.
- 2 Click the **Policy Editor** icon  in the actions toolbar, then click **Tools | Compare Rule Files**.
- 3 On the **Compare Rules Files** page, make the selections, then click **Compare**.

If both of the resulting files are less than about 15.5 MB, they appear in the **Compare Rules Files** table. If either of the files is larger, you are prompted to download both files.

View the rule change history

You can view the rules that were changed, updated, or added to the system, as well as the latest version of each rule.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the **Policy Editor**, click **Tools | Rule Change History**.
- 2 On the **Rule History** page, view the changes made to rules, or click the **Rule Version** tab to see the latest version of each rule.
- 3 Click **Close**.

Table 12-40 Option definitions

Option	Definition
Rule Change History	View the recent rule changes. Each entry gives a summary of the rule and the date it was updated or added to the system.
Rule Version	View the newest time stamp for each device that rules are categorized under on the system. This provides you with a way to locate the version of each rule for management and compliance regulations. By default, the device types are sorted alphabetically by name. To sort them by time stamp, click the Version column header.
Show All	On the Rule Change History tab, click to generate a list of all rule changes, not just recent ones.

Create a new watchlist of rules

A watchlist is a grouping of specific types of information that can be used as filters or as an alarm condition so you are notified when they occur in an event. These watchlists can be global or specific to an ESM user or group.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule, then select the rules that you want to have on this watchlist.
- 2 Click **Operations**, then select the **Create new watchlist** option.
The **Add Watchlist** page lists the rules you selected.
- 3 Type a name, then make sure the **Static** radio button is selected.



See *Add a new watchlist* to add a dynamic watchlist.

- 4 Select the type of data this watchlist is watching for, then select the assignee.



A user with administrator privileges can assign a watchlist to anyone or any group on the system. If you do not have administrator privileges, you can only assign watchlists to yourself and groups you are a member of.

- 5 To add more values to the watchlist, you can do so in the following ways:
 - To import a file of values in new-line-separated values format, click **Import**, then select the file.
 - To add individual values, type one value per line in the **Values** box.



Maximum number of values is 1000.

- 6 To receive an alarm when an event is generated that contains any of the values on this watchlist, click **Create Alarm**.
- 7 Click **OK**.

Add rules to a watchlist

After creating a watchlist, you might need to add rule values to it. The **Append to watchlist** option provides a way for you to do that.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule.
- 2 Select the rules you want to append to the watchlist in the rule display pane.
- 3 Click the **Operations** menu, then select **Append to watchlist**.
- 4 Select the watchlist you want to append the rules to, and click **OK**.

Table 12-41 Option definitions

Option	Definition
Top table	Lists the values for the rules you selected to append to the watchlist.
Bottom table	Select the watchlist where you want to append the values.

Assign tags to rules or assets

You can assign tags to rules, indicating their attributes, and then filter the rules by their tags. The ESM has a predefined set of tags but also provides you with the ability to add new tags and new tag categories.

The **Tags** tab is not available for Variable, Preprocessor, or Normalization rule types.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule you want to tag.
- 2 Click the **Tags** tab in the **Filters/Tagging** pane.
- 3 Do any of the following:





To...	Do this...
Add a new tag category	<ol style="list-style-type: none"> 1 Click the New Category Tag icon . 2 Type the name for the category. 3 If you want this tag to be used in event severity calculation, select Use tag for event severity calculation, then click OK. <p>The category is added with a base tag. You can add new tags under this category.</p>
Add a new tag	<ol style="list-style-type: none"> 1 Click the category you want to add the tag to, then click the New Tag icon . 2 Type the name for the tag. 3 If you want this tag to be used in event severity calculation, select Use tag for event severity calculation, then click OK.
Edit an existing category or tag	<ol style="list-style-type: none"> 1 Click the category or tag you want to edit, then click the Edit Tag icon . 2 Change the name or setting, then click OK.
Delete a custom tag	<ol style="list-style-type: none"> 1 Highlight the tag you want to delete, then click the Remove Tag icon . 2 Click Yes to confirm.

Table 12-42 Option definitions

Option	Definition
Search field	If you are searching for a specific tag, type it in the field, then select it from the list of possible matching tags.
Table of tags	View and search through the tags available on the system.

Modify aggregation settings

Aggregated events are events that have fields that match.

Aggregation is selected by default and you can choose the type of aggregation to be used for all events generated on a device on the **Event Aggregation** page for each device. You can modify the aggregation settings for individual rules.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule.
- 2 Select the rule for which you want to modify aggregation settings.
- 3 Click **Operations** on the toolbar and select **Modify Aggregation Settings**.
- 4 Select the field types you want to aggregate from the **Field 2** and **Field 3** drop-down lists.



The fields you select must be different types or an error results.

- 5 Click **OK** to save the settings.

- 6 If you made changes that affect the way devices aggregate, you are asked if you want to roll out the changes. Do the following:

- a Click **Yes**.

The **Aggregation Exceptions Rollout** page shows the status of the devices affected by this change. All devices that are out of date are checked.

- b If needed, deselect the checkmark from the devices you do not want to apply the changes to.
- c Click **OK** to roll out the changes.

The **Status** column reflects the status of the update as the changes are rolled out.

Table 12-43 Option definitions

Option	Definition
Field 2 and Field 3	Select the field types you want to aggregate. They must be different types. The descriptions for level 1, level 2, and level 3 aggregation changes based on your selections

Override action on downloaded rules

When rules are downloaded from the central server at McAfee, they have a default action assigned to them. You can define an override action for rules of the type that you select when they are downloaded. If there is no override action defined, the rules take their default action.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the **Policy Editor**, click **Tools**, then select **New Rule Configuration**.

The **New Rule Configuration** page lists overrides that exist for the **Default Policy**.

- 2 Set the override action settings, then click **Close**.

Table 12-44 Option definitions

Option	Definition
Policy	Select the policy for the rule you want to apply the override to.
Table	View the existing overrides for the selected policy.
Add	Click to add an override to the selected policy.
Edit	Change the settings for the selected override.
Delete	Delete the selected override.

Table 12-45 Option definitions

Option	Definition
List of tags	Select the tags assigned to the rule where you want to apply this override. For example, to override the action for all filter rules with the AOL tag, click Current Threats AOL in the tags list, then select Filter in the Rule Type field.
Rule Type field	Select the rule type that you want this override to apply to.
Rule Action	Select to have this rule and tag continue to use the default setting, if you want to enable the override, or if you want to disable this rule and tag.

Table 12-45 Option definitions *(continued)*

Option	Definition
Severity	Select the severity for this override. The default is zero.
Blacklist, Aggregation, Copy Packet	Select the settings for this override. If you don't want the settings for these options to be overridden, keep the settings at default .

Severity weights

Event severity is calculated based on the severity weight given to assets, tags, rules, and vulnerabilities.

Each of the four severities is weighted in the final calculation. This final calculation is the sum of each of the four severities multiplied by their respective weights. The **Severity Weights** page shows the weights that are associated with the assets, tags, rules, and vulnerability groups. The sum of the settings must equal 100. When you change one setting, some or all other settings are affected. Here is a description of each type of severity:

Severity type	Descriptions
Asset	<p>An asset is an IP address, optionally within a zone. The asset severity of an event is determined as follows:</p> <ol style="list-style-type: none"> 1 The destination IP address and destination zone of the event are compared against all assets. If a match is found, the severity of that asset is used as the asset severity for this event. 2 If no destination IP address and destination zone match is found, the source IP address and source zone of the event are compared against all assets. If a source IP address and source zone match is found, the severity of the asset is used as the asset severity for this event. 3 If no matches are found, the asset severity is zero.
Tag	The tag severity is calculated using both McAfee and user-defined tags. For a tag to be used in the severity calculation, it must be set for both the rule and asset of the event. If the rule or asset does not have any tags defined or if there were no asset matches, the tag severity is zero. To calculate the tag severity, the number of matching rule and asset tags is multiplied by 10. The tag severity is limited to 100.
Rule	The rule severity is the severity set for the event when it was created. It is based on the event's rule severity, as set in the Policy Editor , and any data enrichment configured for the event's collector.
Vulnerability	If VA SVE information is available for an event's asset and rule, then the highest severity of all matching asset and rule VA SVEs is used for the vulnerability severity, otherwise zero it used.

See also

[Set the severity weights on page 412](#)

Set the severity weights

Asset, tag, rule, and vulnerability severities are weighted when calculating event severity. You must define these severities.

Task

For details about product features, usage, and best practices, click **?** or **Help**.


- 1 On the **Policy Editor**, click the **Severity Weights** icon .
- 2 Define the settings, then click **OK**.

Table 12-46 Option definitions

Option	Definition
Number line	Drag and drop the markers. The Assets , Tags , Rules , and Vulnerability fields reflect these settings.
VA vendor-provided severity or VA vendor-provided PCI severity	Select how the vulnerability severity should be calculated on incoming data. If you select both, the greater of the two values is used when calculating the severity value.

See also

[Severity weights](#) on page 412

View policy change history

You can view or export a log of the changes that have been made to the policy. This log can hold a maximum of 1GB of data. When it reaches this limit, the oldest files are deleted as needed.

Task

For details about product features, usage, and best practices, click ? or **Help**.


- 1 On the **Policy Editor**, click the **View Policy Change History** icon .
- 2 View or export a log, then click **Close**.

Table 12-47 Option definitions


Option	Definition
Table	View a list of the changes that have been made to the current policy
View	View the details for the selected log. If you want to download these details, click Download Entire File .
Export	Export the details of the selected log.

Apply policy changes

When you make changes to policies, you must roll out the changes to apply them. Changes made at the default policy level are applied to all policies when you roll out to all devices.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the **Policy Editor**, click the **Rollout** icon .
- 2 Select how you want the rollout to occur.
- 3 Click **OK**.

After each device completes the rollout, the status of the policy will indicate a successful rollout. If the rollout command was unsuccessful, a page shows a summary of the failed commands.

Table 12-48 Option definitions


Option	Definition
	Click to roll out the policy to one device.
Rollout policy to all devices now	Select to roll out the policy changes to all the devices. Click OK .
Edit	Click to select other roll out options.

Table 12-49 Option definitions

Option	Definition
Stage rollout for later	Select to set a future time to rollout the policy for the devices you selected on the Rollout page. Click the calendar icon to set the date and time.
Rollout now	Select to roll out the policy to the selected devices now.
Roll device back to previous active policy	If it is enabled, select to go back to the previously applied policy.
Skip or Clear staged policies	Select to skip the staged rollout for this device.

See also

[Understanding the Policy Editor on page 355](#)

[The Policy Tree on page 357](#)

[Rule types and their properties on page 361](#)


[Manage policies on the Policy Tree on page 357](#)

Enable Copy Packet

When **Copy Packet** is enabled for a rule, the packet data is copied to the ESM. If enabled, packet data is included within the source event data of an **Internal Event Match** or **Field Match** alarm.

Task

For details about product features, usage, and best practices, click **?** or **Help**.

- 1 On the ESM console, click the **Policy Editor** icon .
- 2 In the **Rule Types** pane, click the type of rule that you want to access, then locate the rule in the rule display pane.
- 3 Click the current setting in the **Copy Packet** column, which is **off** by default, then click **on**.



FIPS mode information

Contents

- ▶ [FIPS mode information](#)
- ▶ [Check FIPS integrity](#)
- ▶ [Adding a keyed device in FIPS mode](#)
- ▶ [Troubleshooting FIPS mode](#)

FIPS mode information

Due to FIPS regulations, some ESM features aren't available, some available features are not compliant, and some features are only available when in FIPS mode. These features are noted throughout the document and are listed here.

Feature status	Description
Removed features	<ul style="list-style-type: none">• High availability Receivers.• Ability to communicate with the device using SSH protocol.• On the device console, a device management menu replaces the root shell.
Features available only in FIPS mode	<ul style="list-style-type: none">• Four user roles do not overlap: User, Power User, Audit Admin, and Key & Certificate Admin.• All Properties pages have a Self-Test option that allows you to verify that the system is operating successfully in FIPS mode.• If FIPS failure occurs, a status flag is added to the system navigation tree to reflect this failure.• All Properties pages have a View option that, when clicked, opens the FIPS Identity Token page. It displays a value that must be compared to the value shown in those sections of the document to ensure that FIPS hasn't been compromised.• On System Properties Users and Groups Privileges Edit Group, the page includes the FIPS Encryption Self Test privilege, which gives the group members the authorization to run FIPS self-tests.• On the Add Device Wizard, TCP protocol is always set to Port 22. The SSH port can be changed.

See also

[Check FIPS integrity on page 416](#)

[Adding a keyed device in FIPS mode on page 417](#)

[Back up and restore information for a device in FIPS mode on page 417](#)

[Enable communication with multiple ESM devices in FIPS mode on page 418](#)

[Troubleshooting FIPS mode on page 419](#)

Check FIPS integrity

If you are operating in FIPS mode, FIPS 140-2 requires software integrity testing regularly. This testing must be performed on the system and each device.

Task

For details about product features, usage, and best practices, click ? or **Help**.

- 1 On the system navigation tree, select **System Properties**, and make sure that **System Information** is selected.
- 2 Do any of the following.

In this field...	Do this...
FIPS Status	View the results of the most recent FIPS self-test performed on the ESM.
Test or FIPS Self-Test	Run the FIPS self-tests, which test the integrity of the algorithms used in the crypto-executable. The results can be viewed on the Message Log . <div>  If the FIPS self-test fails, FIPS is compromised or device failure is occurring. Contact McAfee Support. </div>
View or FIPS Identity	Open the FIPS Identity Token page to perform power-up software integrity testing. Compare this value to the public key that appears on this page: <div> <p>-----BEGIN PUBLIC KEY-----</p> <pre> MIICljANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAGEA8tFWOP2mvVjvTTxkhGqk LdgA+sx0jBv+zYnCKGYOHHzNAdum9yuMn69GNbYXm7I5OcKv2+nz6axBruCZ5XX1 jCGWnmsj8YZJoNp/FLUy1jYE7lXI5/NRm2uhjhzjdOjgFv10SkgxVfL/aBJjqZFJ KKbHMzYEBwdyseQUc56u3mKaBtP4rydRmEtytkuOsZgQuPHKYhaQJlnbV5LfrLa o6HQSlzHYHlcF/Yog+QHJ6ClSRA1lk8MPyFG9RHdKnwcq3sY8QjQMbIZSSDobbK0 GPOOucG8vWDWdxSiabJLBdklVsmB0zwdH6lOCkkGTidayMk12hDh+2BA6e17YQBV 8EJaJ5wvz8aQKwDfiinlb9vmC+sk+Rwo/E7uRn3El4+RxouHi9J3f92I9qXZeJCV iYV2XahhyxSpq8ro/j0BMTiab3dIjjogxMxCI9QjEpm3J/ZyUpWtNkaHq8BgSE1e daiJob7O/kvef1T/ZOb3O90bSK3vtr+3Si3K3cpaY/qBm9var6xVNyGhHztRjv0F 0nSJlyddWuXL1U+hMTO2YE33T3s4Uf4jiomTVSDTJ087hLT5l/hCz6A33Hzl7gk8 Q89SNsmL/p0RAJzJ3+mGyoUAd1D2u6sYq6NkGCn640a5A2zAOQdX/M8R8S+NKjgi nLg3n+/+25KsCB3KDY3AkYECaWEAAQ== -----END PUBLIC KEY----- </pre> <div>  If this value and the public key don't match, FIPS is compromised. Contact McAfee Support. </div> </div>

See also

[FIPS mode information on page 415](#)

[Adding a keyed device in FIPS mode on page 417](#)

[Back up and restore information for a device in FIPS mode on page 417](#)

[Enable communication with multiple ESM devices in FIPS mode on page 418](#)

[Troubleshooting FIPS mode on page 419](#)

Adding a keyed device in FIPS mode

There are two methods in FIPS mode to add a device that has already been keyed to an ESM. This terminology and file extensions are useful as you follow these processes.

Terminology

- **Device key** — Contains the management rights that an ESM has for a device, and is not used for crypto.
- **Public key** — The ESM public SSH communication key, which is stored in the authorized keys table of a device.
- **Private key** — The ESM private SSH communication key, which is used by the SSH executable on an ESM to establish the SSH connection with a device.
- **Primary ESM** — The ESM that was originally used to register the device.
- **Secondary ESM** — The additional ESM that communicates with the device.

File extensions for the different export files

- **.exk** — Contains the device key.
- **.puk** — Contains the public key.
- **.prk** — Contains the private key and the device key.

See also

[FIPS mode information on page 415](#)

[Check FIPS integrity on page 416](#)

[Back up and restore information for a device in FIPS mode on page 417](#)

[Enable communication with multiple ESM devices in FIPS mode on page 418](#)



[Troubleshooting FIPS mode on page 419](#)

Back up and restore information for a device in FIPS mode

This method is used to back up and restore communication information for a device on the ESM.

Primarily, you can use it in the event of a failure that requires ESM replacement. If the communication information is not exported before the failure, communication with the device can't be re-established. This method exports and imports the .prk file.

The private key for the primary ESM is used by the secondary ESM to establish communication with the device initially. Once communication is established, the secondary ESM copies its public key to the device's authorized keys table. The secondary ESM then erases the private key for the primary ESM, and initiates communication with its own public or private key pair.

Action	Steps
Export the .prk file from the primary ESM	<ol style="list-style-type: none"> 1 On the system navigation tree of the primary ESM, select the device with communication information you want to back up, then click the Properties icon. 2 Select Key Management, then click Export Key. 3 Select Backup SSH Private key, then click Next. 4 Type and confirm a password, then set the expiration date. <div>  <p>After the expiration date passes, the person who imports the key is unable to communicate with the device until another key is exported with a future expiration date. If you select Never Expire, the key never expires if imported into another ESM.</p> </div> 5 Click OK, select the location to save the .prk file created by the ESM, then log off of the primary ESM.
Add a device to the secondary ESM and import the .prk file	<ol style="list-style-type: none"> 1 On the system navigation tree of the secondary device, select the system or group level node you want to add the device to. 2 From the actions toolbar, click Add Device. 3 Select the type of device that you want to add, then click Next. 4 Enter a name for the device that is unique in this group, then click Next. 5 Enter the target IP address of the device, enter the FIPS communication port, then click Next. 6 Click Import Key, browse to the previously exported .prk file, then click Upload. <div>  <p>Type the password specified when this key was initially exported.</p> </div> 7 Log off of the secondary ESM.

See also

[FIPS mode information on page 415](#)

[Check FIPS integrity on page 416](#)

[Adding a keyed device in FIPS mode on page 417](#)

[Enable communication with multiple ESM devices in FIPS mode on page 418](#)

[Troubleshooting FIPS mode on page 419](#)

Enable communication with multiple ESM devices in FIPS mode

You can allow multiple ESMs to communicate with the same device by exporting and importing .puk files.

The primary ESM is used to import the secondary ESM device exported .puk file and send the contained secondary ESM public key to the device, thus allowing both ESM devices to communicate with the device.

Action	Steps
Export the .puk file from the secondary ESM	<ol style="list-style-type: none"> 1 On the System Properties page of the secondary ESM, select ESM Management. 2 Click Export SSH, then select the location to save the .puk file. 3 Click Save, then log off.
Import the .puk file to the primary ESM	<ol style="list-style-type: none"> 1 In the system navigation tree of the primary ESM, select the device you want to configure. 2 Click the Properties icon, then select Key Management. 3 Click Manage SSH Keys. 4 Click Import, select the .puk file, then click Upload. 5 Click OK, then log off of the primary ESM.

See also

[FIPS mode information on page 415](#)

[Check FIPS integrity on page 416](#)

[Adding a keyed device in FIPS mode on page 417](#)

[Back up and restore information for a device in FIPS mode on page 417](#)

[Troubleshooting FIPS mode on page 419](#)

Troubleshooting FIPS mode

Issues might arise when operating the ESM in FIPS mode.

Issue	Description and resolution
Can't talk to the ESM	<ul style="list-style-type: none"> • Check the LCD on the front of the device. If it says FIPS Failure, contact McAfee Support. • Check for an error condition through the HTTP interface by viewing the ESM FIPS Self-test webpage in a browser. <ul style="list-style-type: none"> - If a single digit 0 is displayed, indicating that the device has failed a FIPS self-test, reboot the ESM device and attempt to correct the problem. If the failure condition persists, contact Support for further instructions. - If a single digit 1 is displayed, the communication problem is not due to FIPS failure. Contact Support for further troubleshooting steps.
Can't talk to the device	<ul style="list-style-type: none"> • If there is a status flag next to the device on the system navigation tree, place the cursor over it. If it says FIPS Failure, contact McAfee Support by going to the support portal. • Follow the description under the <i>Can't talk to the ESM</i> issue.
The file is invalid error when adding a device	You cannot export a key from a non-FIPS device and then import it to a device operating in FIPS mode. Also, you cannot export a key from an FIPS device and then import it to a non-FIPS device. This error appears when you attempt either scenario.

See also

[FIPS mode information on page 415](#)

[Check FIPS integrity on page 416](#)

[Adding a keyed device in FIPS mode on page 417](#)

[Back up and restore information for a device in FIPS mode on page 417](#)

[Enable communication with multiple ESM devices in FIPS mode on page 418](#)

Index

A

- about this guide [9](#)
- access control list, set up [197](#)
- access, grant to devices [35](#)
- accumulator indexes, increase available [188](#)
- accumulator indexing, manage [190](#)
- ACE
 - add a risk correlation manager [112](#)
 - correlation engine [111](#)
 - correlation engines [111](#)
 - historical correlation [116](#)
 - risk correlation engine [111](#)
 - risk correlation scoring, add [114](#)
 - select data type to send from ESM [111](#)
 - summary [14](#)
- acknowledge
 - triggered alarm [251](#)
- actions
 - add to DEM [137](#)
 - alarms [246](#)
 - data sources [75](#)
 - define for DEM [136](#)
 - maps [75](#)
- Active Directory
 - configure authentication settings [199](#)
 - login authentication [195](#)
 - retrieve data [341](#)
- Active Response [322](#)
 - data validation, watchlist [322](#)
 - date format [322](#)
 - DXL [322](#)
- Active Response search results
 - append data to a watchlist [323](#)
 - create watchlist [323](#)
 - export data [323](#)
 - search on resulting data [323](#)
- add a subzone [347](#)
- Adiscon data source setup [83](#)
- ADM
 - events [117](#)
 - settings [117](#)
 - summary [14](#)
- ADM dictionaries [119](#)
 - examples [122, 370](#)
- ADM dictionaries [119](#) (*continued*)
 - manage [123](#)
 - referencing [121](#)
 - setting up [120](#)
- ADM rules
 - add new [364](#)
 - DNA protocol anomalies for ADM rules [132, 377](#)
 - email protocol modules [131, 376](#)
 - file transfer protocol modules [131, 376](#)
 - IP protocol anomalies for ADM rules [132, 377](#)
 - key concepts [362](#)
 - literals [124, 368](#)
 - logic elements [264](#)
 - logical elements, edit [367](#)
 - manage custom [364](#)
 - metric references [129, 374](#)
 - operators [124, 368](#)
 - protocol anomalies [132, 377](#)
 - protocol-specific properties [131, 376](#)
 - REGEX grammar [124, 368](#)
 - supported applications and protocols [362](#)
 - syntax [124, 368](#)
 - TCP protocol anomalies for ADM rules [132, 377](#)
 - term types [127, 372](#)
 - web mail protocol modules [131, 376](#)
- ADM session viewer, display passwords [119](#)
- administrative roles
 - UCAPL, alarm [254](#)
- advanced DEM settings, configure [134](#)
- advanced syslog parser
 - add custom rule [379](#)
 - data sources [76](#)
 - rules [378](#)
- advanced syslog parser data source
 - encoding other than UTF-8 [80](#)
- aggregation
 - add exceptions [277](#)
 - manage event exceptions [278](#)
 - modify rule settings [410](#)
 - settings for device [276](#)
 - what is it [275](#)
- alarm
 - manage queries [217](#)
 - watchlist, update with alarm data [304](#)

- alarms [239](#)
 - acknowledge [250](#), [251](#)
 - actions [246](#)
 - add to rule [265](#)
 - add watchlist to Internal Event Match alarm [301](#)
 - assignee [246](#), [251](#)
 - assignee, change [251](#)
 - audio alerts [244](#)
 - audio files [244](#)
 - build [239](#), [244](#)
 - cases [251](#)
 - conditions [246](#)
 - copy [245](#)
 - correlation events [241](#)
 - create [246](#), [253](#)
 - customize summary [265](#)
 - delete [251](#)
 - disable [245](#)
 - edit [251](#)
 - email [239](#)
 - enable [245](#), [246](#)
 - escalation [246](#)
 - filter [251](#)
 - health monitor signature IDs [256](#)
 - mail server, messages [157](#)
 - message recipients [243](#)
 - message templates [240](#)
 - messages [156](#)
 - messages, mail server [157](#)
 - messages, setup [239](#)
 - monitor [250](#)
 - notifications, add recipients [157](#)
 - pane, show [193](#)
 - power failure [266](#)
 - recipients [243](#)
 - reports [252](#)
 - response [250](#)
 - severity [246](#)
 - SMS [239](#)
 - SNMP [239](#)
 - source events, correlation [241](#)
 - syslog [239](#)
 - templates [240](#)
 - Threat Intelligence Exchange alarms [148](#)
 - tuning [253](#)
 - UCAPL, create [254](#)
 - view [250](#)
 - workflow [239](#)
 - alerts
 - alarms escalation [246](#)
 - aliases, add [167](#)
 - allocation, define data limits [189](#)
 - Altiris server, retrieve data [341](#)
 - apply configuration settings to DEM [136](#)
 - archive
 - set up inactive partitions [186](#)
 - settings, define for Receiver [50](#)
 - ArcSight, add data source [82](#)
 - ASN
 - define settings for device [274](#)
 - lookup, perform [309](#)
 - ASP [378](#)
 - ASP rules
 - set order [382](#)
 - time formats, add [383](#)
 - asset manager [348](#)
 - asset sources [341](#)
 - add Receiver [88](#)
 - manage [341](#)
 - Receiver [88](#)
 - assets
 - define old assets [340](#)
 - manage [338](#)
 - severity [412](#)
 - assignee
 - alarms escalation [246](#)
 - audio files
 - alarms [244](#)
 - upload [244](#)
 - audits
 - UCAPL, alarm [254](#)
 - authentication for ePO [146](#)
 - auto create data sources [63](#)
 - auto create data sources rules, add [63](#)
 - auto learning data sources, set up [64](#)
 - auto-acknowledge
 - alarms action [246](#)
 - auto-learned data source rules, manage [393](#)
- ## B
- back up
 - ELM [104](#)
 - ESM settings [206](#)
 - system settings [206](#)
 - back up, restore [208](#)
 - backup files, work with [209](#)
 - bind components
 - link components [229](#)
 - blacklist
 - add McAfee Network Security Manager entry [152](#)
 - entry, add or delete removed McAfee Network Security Manager [153](#)
 - global [218](#)
 - set up global [219](#)
 - blacklists
 - alarms action [246](#)
 - build, view software [25](#)

C

- CA root certificate, upload [198](#)
- CAC
 - add users [198](#)
 - authentication [195](#)
 - login, set up [198](#)
 - settings [197](#)
 - upload CA root certificate [198](#)
- case management
 - pane, show [193](#)
 - reports, generate [334](#)
- cases
 - add [327](#)
 - add events to an existing case [328](#)
 - alarms action [246](#)
 - close [330](#)
 - create from triggered alarm [251](#)
 - customize summary [265](#)
 - edit [330](#)
 - email notification [333](#)
 - email selected case [333](#)
 - filter [333](#)
 - reports, generate [334](#)
 - send email when add or change [333](#)
 - source events, view [333](#)
 - status, add [332](#)
 - status, add or edit [333](#)
 - view all [333](#)
 - view details [331](#)
- category
 - add new tag [409](#)
 - add new variable [398](#)
 - edit [409](#)
- certificates
 - UCAPL, alarm [254](#)
- certificate
 - install new [176](#)
 - passphrase, obtain McAfee Vulnerability Manager [151](#)
- certificate, upload CA root for CAC [198](#)
- change history, view for rules [408](#)
- Check Point data sources, set up [86](#)
- check rate
 - alarms condition [246](#)
- child data sources, add [67](#)
- client data sources [68](#)
 - add [68](#)
 - locate [69](#)
- clock, sync device [176](#)
- Collector
 - SIEM Collector [56](#)
- common event format data sources [82](#)
- compare rule files [407](#)
- comparing values on distribution graphs [314](#)
- components
 - add parameters to [390](#)
- components (*continued*)
 - bind [229](#)
 - example of rule [387](#)
 - export [310](#)
 - image, add [291](#)
 - view [308](#)
- compression, managing ELM [103](#)
- compression, set ELM [104](#)
- concurrent sessions
 - UCAPL, alarm [254](#)
- condition, add report [292](#)
- conditions
 - alarms [246](#)
 - check rate [246](#)
 - deviation [246](#)
 - event rate [246](#)
 - field match [246](#)
 - health monitor [246](#)
 - internal event match [246](#)
 - threshold [246](#)
 - trigger frequency [246](#)
- configuration files, sync DEM [134](#)
- configuration settings, apply to DEM [136](#)
- connections
 - change with ESM [35](#)
 - set up McAfee Vulnerability Manager [152](#)
- console
 - add device [21](#)
 - change appearance [193](#)
 - timeout [22](#)
- contains filter [293](#)
- conventions and icons used in this guide [9](#)
- copy and paste rules [402](#)
- correlation data sources [74](#)
- correlation engine, ACE [111](#)
- correlation event, view source events [51](#)
- correlation events
 - alarms, source events [241](#)
 - source events, alarms [241](#)
- correlation manager, add [112](#)
- correlation rules [387](#)
 - add new [364](#)
 - add parameters [390](#)
 - conflicts when importing [403](#)
 - example [387](#)
 - logic elements [264](#)
 - logical elements, edit [367](#)
 - manage custom [364](#)
 - Threat Intelligence Exchange rules [148](#)
 - view details
 - set to show details [389](#)
- create
 - alarms [239](#)
- credentials for ePO [146](#)
- credentials, obtain, and add rule update [19](#)

- custom
 - type filters [317](#)
- custom ASP rules, add [379](#)
- custom display, add, edit, delete [22](#), [40](#)
- custom rules
 - view [402](#)
- custom type
 - add name/value group [321](#)
- custom types
 - add time [320](#)
 - create [319](#)
 - name/value [320](#)
 - predefined [320](#)
- customer ID [155](#)
- customize summary [265](#)
- cyber threat feed
 - manual upload errors [236](#)
- cyber threat feeds [235](#)

D

- DAS, assign to store ELM data [100](#)
- data access rules, add or edit [393](#)
- data acquisition
 - enable McAfee Risk Advisor [147](#)
 - McAfee Risk Advisor [147](#)
- data allocation, define limits [189](#)
- data enrichment [220](#)
 - Active Response
 - add data enrichment source [324](#)
 - Active Response search results [324](#)
 - add sources [221](#)
 - query ePO devices [150](#)
- data retention limits, set up [189](#)
- data source
 - out-of-sync with ESM [267](#)
- data source rules [392](#)
 - auto-learned, manage [393](#)
- data sources [52](#)
 - add [53](#)
 - add ArcSight [82](#)
 - add child [67](#)
 - Adiscon setup [83](#)
 - advanced syslog parser [76](#)
 - ASP encoding [80](#)
 - auto create [63](#)
 - auto create rules, add [63](#)
 - auto learning, set up [64](#)
 - Check Point, set up [86](#)
 - client [68](#)
 - client, add [68](#)
 - client, locate [69](#)
 - collection method, tail file [72](#)
 - common event format [82](#)
 - correlation [74](#)
 - encoding for ASP [80](#)
- data sources [52](#) (*continued*)
 - IBM ISS SiteProtector [85](#)
 - import a list [69](#)
 - manage [55](#)
 - McAfee ePO [85](#)
 - migrate to another Receiver [71](#)
 - move to another system [71](#)
 - Security Device Event Exchange (SDEE) [81](#)
 - severity and actions maps [75](#)
 - show disabled [193](#)
 - syslog relay support [83](#)
 - tail file collection method [72](#)
 - time out of sync with ESM [267](#)
 - Windows security logs [74](#)
 - WMI event log [74](#)
- data sources, rule actions [393](#)
- data storage
 - set up ESM [187](#)
 - set up ESM VM [188](#)
 - virtual local drive [101](#)
- data storage, add ELM mirrored [97](#)
- data storage, mirroring ELM [97](#)
- data storage, preparing to store ELM data [91](#)
- database
 - audit trails [360](#)
 - audit trails, set up rule and report [360](#)
 - manage [186](#)
 - manage index settings [190](#)
 - memory utilization [191](#)
 - server, add [142](#)
 - status [155](#)
- database migration
 - virtual local drive [101](#)
- database rules
 - add new [364](#)
 - logic elements [264](#)
 - logical elements, edit [367](#)
- date format, change [193](#)
- default display type, change [193](#)
- default logging pool, set [34](#)
- default view, change [316](#)
- delete
 - custom rules [402](#)
 - triggered alarm [251](#)
- DEM
 - add action [137](#)
 - advanced settings, configure [134](#)
 - configuration settings, apply [136](#)
 - database server, add [142](#)
 - define actions [136](#)
 - edit custom action [137](#)
 - rules [394](#)
 - sensitive data masks [139](#)
 - set operation [138](#)
 - summary [14](#)

DEM (continued)

- sync configuration files [134](#)
- update license [134](#)
- user identification [140](#)

DEM rules

- manage custom [364](#)

DEM-specific settings [133](#)destination IP addresses, show host name in report [292](#)

deviation

- alarms condition [246](#)

device display type, select [21](#)device group, manage [40](#)device nodes, delete duplicate [41](#)

device time

- view for event [300](#)

devices

- add device [21](#)
- add to console [21](#)
- add URL link [27](#), [31](#)
- aggregation settings [276](#)
- ASN, define settings [274](#)
- build [25](#)
- change default display [193](#)
- change description [29](#)
- change name [29](#)
- connection with ESM, change [35](#)
- control network traffic [32](#)
- count report [155](#)
- delete nodes [41](#)
- device statistics [29](#)
- disable data sources [193](#)
- geolocation, define settings [274](#)
- grant access to [35](#)
- group node, delete [41](#)
- IPMI port, set up [168](#)
- key [23](#)
- machine ID [25](#)
- manage keys [23](#)
- manage multiple [31](#)
- manage SSH communication keys [24](#)
- message log [29](#)
- model [25](#)
- NTP servers [158](#)
- organize [22](#), [25](#), [40](#)
- reboot [35](#)
- refresh [30](#)
- serial number [25](#)
- set up events, flows, and logs downloads [270](#)
- start [35](#)
- status data, download [29](#)
- stop [35](#)
- summary reports [30](#)
- sync clocks [176](#)
- sync with ESM [33](#)
- version [25](#)

devices (continued)

- view general information [25](#)
- view log [30](#)

DHCP, set up [174](#)disable ELM mirroring device [98](#)disable SSH communication with ESM [35](#)display type, select [21](#)

distributed ESM

- add filters [145](#)
- properties [144](#)

distribution graph, compare values [314](#)DNA protocol anomalies for ADM rules [132](#), [377](#)

documentation

- audience for this guide [9](#)
- product-specific, finding [10](#)
- typographical conventions and icons [9](#)

download

- events, flows, and logs [270](#)

downloaded rules, override action [411](#)duplicate device nodes, delete [41](#)**E**

ELM

- add iSCSI device for storage [99](#)
- add mirrored data storage [97](#)
- add storage device [94](#)
- back up [104](#)
- compression [103](#)
- compression, set [104](#)
- DAS device to store ELM data [100](#)
- define alternate storage location [106](#)
- disable mirroring device [98](#)
- external data storage [98](#)
- format SAN storage device to store data [99](#)
- integrity check job [107](#)
- integrity check job, create [108](#)
- integrity check, view results [109](#)
- log data, restore [105](#)
- management database, restore [105](#)
- migrating database [106](#)
- mirrored data storage, add [97](#)
- mirrored management database, replace [107](#)
- mirrored storage pool, rebuild [98](#)
- mirroring data storage [97](#)
- move storage pool [96](#)
- preparing to store data [91](#)
- query using regex [110](#)
- restore [104](#)
- retrieve data [107](#)
- search job [107](#)
- search job, create [108](#)
- search job, view results [109](#)
- search view [307](#)
- search, enhanced [307](#)
- set up communication with [33](#)

ELM (*continued*)

- storage allocation, reduce [97](#)
- storage pool, add or edit [95](#)
- storage usage, view [106](#)
- store logs [93](#)
- summary [14](#)
- sync with device [33](#)

ELM redundancy

- return standby ELM to service [101](#)
- suspend communication with standby ELM
 - disable redundancy [101](#)
 - view details of data synchronization [101](#)
- switch ELMs [101](#)

ELM settings [90](#)ELM storage, estimating need [90](#)

email

- alarms [239](#)
- case notification [333](#)
- mail server, connect [157](#)

email protocol modules for ADM rules [131](#), [376](#)enable FIPS mode [17](#)encoding for ASP data source [80](#)

ePO

- add authentication credentials [146](#)
- streaming events, view [43](#)

ePO authentication credentials [146](#)

ePO devices

- query for data enrichment [150](#)
- query for reports or views [150](#)

ePO tag

- alarms action [246](#)

ePolicy Orchestrator

- launch from ESM [145](#)
- McAfee Risk Advisor data acquisition, enable [147](#)
- settings [145](#)
- tags, assign to IP address [147](#)

escalation

- alarms [246](#)

ESM

- back up settings [206](#)
- backup files [209](#)
- control network traffic [170](#)
- data storage, set up [187](#)
- IPMI port, set up [168](#)
- logging, set up [216](#)
- manage [212](#)
- out-of-sync with data source [267](#)
- redundant ESM [206](#)
- redundant, how it works [210](#)
- replace redundant [211](#)
- restore settings [208](#)
- rules [395](#)
- security features [194](#)
- summary [14](#)
- sync with device [33](#)

ESM (*continued*)

- time out of sync with data source [267](#)
- update software [19](#)
- upgrade primary and redundant [218](#)
- view system information [155](#)

ESM redundancy

- fail-over [212](#)

event forwarding

- add destinations [279](#)
- add filters [282](#)
- agents [281](#)
- configure [279](#)
- edit filter settings [283](#)
- enable or disable [282](#)
- modify settings [282](#)
- setting up [278](#)

event rate

- alarms condition [246](#)

Event Receiver

- summary [14](#)

event time

- view [300](#)

event time report [155](#)

events

- add to a case [328](#)
- alarms escalation [246](#)
- check for [273](#)
- create a case to track [328](#)
- description [269](#)
- log, manage types of events [213](#)
- logs, set language [20](#)
- look around for matching fields [308](#)
- manage aggregation exceptions [278](#)
- retrieve [272](#)
- session details, view [297](#)
- set inactivity threshold [271](#)
- set up downloads [270](#)
- severity weights, set up [412](#)
- view exact time [300](#)

events, flows & logs

- limit collection time [271](#)

exceptions to aggregation settings, add [277](#)

export

- component [310](#)
- rules [404](#)

export and import

- puk file [418](#)

export zones [345](#)

external API

- manage queries [217](#)

external ELM data storage [98](#)**F**fail-over of redundant ESM [212](#)

- failed logons
 - UCAPL, alarm [254](#)
- failed Receiver, replace [49](#)
- field match
 - alarms condition [246](#)
- file extensions for export files [417](#)
- file maintenance, manage [209](#)
- file sharing, disable HomeGroup [93](#)
- file transfer protocol modules for ADM rules [131](#), [376](#)
- filter rules
 - data order [396](#)
 - rule order [396](#)
- Filter rules
 - set order [382](#)
- filter settings, edit event forwarding [283](#)
- filter, contains [293](#)
- filters
 - add rules [396](#)
 - add to distributed ESM [145](#)
 - custom type [317](#)
 - existing rules [404](#)
 - triggered alarm [251](#)
 - UCF [321](#)
 - views [298](#)
 - Windows event ID [321](#)
- filters, event forwarding [282](#)
- filtersnormalized ID, select [299](#)
- FIPS mode
 - backup information [417](#)
 - check integrity [416](#)
 - communicate with multiple ESM devices [418](#)
 - features available only in FIPS mode [415](#)
 - file extensions [417](#)
 - keyed device, add [417](#)
 - non-compliant available features [415](#)
 - removed features [415](#)
 - restore information [417](#)
 - terminology [417](#)
 - troubleshoot [419](#)
- flows
 - check for [273](#)
 - description [269](#)
 - retrieve [272](#)
 - set inactivity threshold [271](#)
 - set up downloads [270](#)
 - views [306](#)

G

- geolocation, define settings for device [274](#)
- global blacklist [218](#)
 - set up [219](#)
- Global Threat Intelligence watchlist [304](#)
- groups
 - set up users [202](#)

- groups (*continued*)
 - users [191](#)
- GTI watchlist [304](#)

H

- Hadoop PIG [225](#)
- hardware [155](#)
- health monitor
 - alarms condition [246](#)
 - signature IDs [257](#)
- health monitor signature IDs
 - alarms [256](#)
- hierarchical ESM, mask data [215](#)
- high-availability Receivers [43](#)
- historical correlation events, download [117](#)
- historical correlation, ACE [116](#)
- historical correlation, add filter [116](#)
- history
 - policy change [413](#)
 - view change for rules [408](#)
- HomeGroup file sharing, disable [93](#)
- host names
 - manage [172](#)
- host names, import list [173](#)
- host names, show in report [292](#)

I

- IBM ISS SiteProtector data source [85](#)
- images
 - add to login page [18](#)
 - include in PDFs and reports [291](#)
- import
 - data sources list [69](#)
 - rules [402](#)
 - string normalization file [317](#)
 - variable [398](#)
- import zone settings [345](#)
- import, host names [173](#)
- inactive partitions archive, set up [186](#)
- inactivity threshold, set [271](#)
- index settings, database [190](#)
- indexes, increase available accumulator [188](#)
- indexing, accumulator [190](#)
- indicator types, supported [235](#)
- indicators of compromise (IOC) [235](#)
- integrity check job [107](#)
 - create [108](#)
- integrity check, view results [109](#)
- interface
 - manage network [164](#)
 - network settings [165](#)
- internal event match
 - alarms condition [246](#)

Internet sources

- create watchlist [304](#)

IP

- address, assign ePolicy Orchestrator tags [147](#)

- IP protocol anomalies for ADM rules [132](#), [377](#)

- IPMI port, configure network [168](#)

- IPMI port, set up on ESM or devices [168](#)

IPv6

- set up Receiver HA [47](#)

- iSCSI device, add for ELM storage [99](#)

K

key

- device [23](#)

- manage device [23](#)

L

- language, set for event logs [20](#)

launch

- ePolicy Orchestrator from ESM [145](#)

- Layer 7, delay pulling events [153](#)

- layout, add report [288](#)

LDAP

- login authentication [195](#)

- server, authenticate users [201](#)

- license, update DEM [134](#)

- limits, set up data retention [189](#)

- literals for ADM rules [124](#), [368](#)

- local drive, virtual [101](#)

- log data, restore ELM [105](#)

log event

- alarms action [246](#)

logging

- console, first time [17](#)

- off console [17](#)

- set the default pool [34](#)

- set up ESM [216](#)

- view system or device [30](#)

- logic elements for ADM, database, correlation rules [264](#)

- logical elements, edit [367](#)

login

- access control list [197](#)

- define settings [195](#)

- security [194](#)

- login page, customize [18](#)

- logo, add to login page [18](#)

logs

- check for [273](#)

- description [269](#)

- manage [213](#)

- set language [20](#)

- set up downloads [270](#)

- logs, store ELM [93](#)

- look around for matching fields in events [308](#)

M

- machine ID, view device [25](#)

mail server,

- alarms, connect [157](#)

- connect [157](#)

- management database, restore ELM [105](#)

- manual upload errors, cyber threat feed

- troubleshoot

- manual upload of IOC STIX XML file [236](#)

- mask IP addresses [215](#)

McAfee ePO

- credentials, set up user [200](#)

- McAfee ePO data sources [85](#)

- McAfee MIB [182](#)

McAfee Network Security Manager

- add or delete [153](#)

- blacklist entry, add [152](#)

- removed blacklist entry [153](#)

- settings [152](#)

McAfee Risk Advisor

- data acquisition [147](#)

- data acquisition, enable [147](#)

- McAfee rulesets [87](#)

- McAfee ServicePortal, accessing [10](#)

McAfee Vulnerability Manager

- certificate and passphrase, obtain [151](#)

- connections, set up [152](#)

- run scans [151](#)

- settings [150](#)

- memory, database utilization [191](#)

- message log, view for device [29](#)

- message settings [156](#)

messages

- alarms [156](#)

- alarms action [246](#)

- alarms escalation [246](#)

- alarms templates [240](#)

- alarms, mail server [157](#)

- alarms, recipients [243](#)

- alarms, setup [239](#)

- email [239](#)

- mail server, connect [157](#)

- recipients, alarms [243](#)

- SMS [239](#)

- SNMP [239](#)

- syslog [239](#)

- metadata events [117](#)

metric references

- ADM rules [129](#), [374](#)

MIB

- pull from ESM [185](#)

- MIB, McAfee [182](#)

- migrate data sources to another Receiver [71](#)

- migrating database, ELM [106](#)

- mirrored data storage, add ELM [97](#)

- mirrored management database, replace ELM [107](#)
- mirrored storage pool, rebuild [98](#)
- mirroring device, disable ELM [98](#)
- mirroring ELM data storage [97](#)
- model, view device [25](#)
- modify rules [402](#)
- monitor
 - alarms [250](#)
- move data sources to another system [71](#)
- move storage pool [96](#)
- multiple devices
 - manage [31](#)

N

- name/value custom types [320](#)
- name/value group custom type, add [321](#)
- network
 - configure settings [160](#)
 - interfaces, set for devices [165](#)
 - manage interfaces [164](#)
- network settings
 - IPMI port set up [168](#)
- network traffic control
 - devices [32](#)
 - ESM [170](#)
- no activity threshold
 - UCAPL, alarm [254](#)
- normalization [361](#)
- normalized ID
 - select [299](#)
- notification, configure SNMP [33](#)
- NSM
 - Layer 7 [153](#)
 - NSM-SIEM configuration tool [84](#)
 - streaming events, view [43](#)
- NTP servers
 - set up for a device [158](#)
 - view status [159](#)

O

- obfuscation [215](#)
- old assets, define [340](#)
- operation, set for DEM [138](#)
- operators for ADM rules [124](#), [368](#)
- out of sync time between ESM and data source [267](#)
- out-of-box views [228](#)
- override action on downloaded rules [411](#)
- oversubscription mode, set up [401](#)

P

- parameters, add to correlation rule or component [390](#)
- partitions, set up inactive archive [186](#)
- passphrase and certificate, obtain McAfee Vulnerability Manager [151](#)

- passwords
 - change [193](#)
 - default [17](#)
- passwords on session viewer, display [119](#)
- PDFs, include image [291](#)
- policy
 - add [357](#)
 - apply changes [413](#)
 - child policy, add [357](#)
 - copy [357](#)
 - delete [357](#)
 - export [357](#)
 - import [357](#)
 - locate [357](#)
 - Policy Tree [357](#)
 - Policy Tree icons [357](#)
 - rename [357](#)
 - view rules [357](#)
- Policy Editor
 - change history [413](#)
 - oversubscription mode, set up [401](#)
 - view update status for devices [401](#)
- power failure
 - alarms [266](#)
- power failure notification [181](#)
- predefined views [228](#)
- primary ESM, upgrade [218](#)
- profiles, configure [177](#)
- protocol
 - anomaly events [117](#)
- protocol anomalies, TCP [400](#)
- protocol-specific properties for ADM rules [131](#), [376](#)

Q

- quarterly reports, set start month [285](#)
- queries
 - delete running [217](#)
 - manage [217](#)
- query CSV reports [156](#)
- Query Wizard [311](#)

R

- RADIUS
 - authentication settings [196](#)
 - login authentication [195](#)
- raw data, archiving [50](#)
- reboot devices [35](#)
- rebuild mirrored storage pool [98](#)
- Receiver
 - asset source, add [88](#)
 - data sources [52](#)
- Receiver-HA [43](#)
 - reinitialize secondary device [46](#)
 - replace failed Receiver [49](#)

- Receiver-HA 43 (*continued*)
 - set up devices 46
 - set up with IPv6 47
 - switch roles 49
 - troubleshoot failure 50
- Receivers
 - archive settings, define 50
 - archiving raw data 50
 - asset sources 88
 - configure settings 42
 - streaming events, view 43
- recipients
 - add 157
 - alarm messages 243
- reduce ELM storage allocation 97
- redundancy fail-over 212
- redundant ESM
 - how it works 210
 - replace 211
 - save system settings 210
 - set up 206
 - upgrade 218
- reference ADM dictionary 121
- refresh devices 30
- refresh system navigation tree, discontinue 156
- REGEX grammar for ADM rules 124, 368
- regex, use to query ELM 110
- reinitialize secondary Receiver-HA device 46
- remedy
 - case ID, add to event record 310
 - server settings 155
- Remedy
 - alarms action 246
- remote command profile, configure 177
- remote commands
 - alarms action 246
 - alarms escalation 246
- removed McAfee Network Security Manager blacklist entry, add or delete 153
- replace failed Receiver-HA 49
- report
 - manage queries 217
- reports
 - add 286
 - add condition 292
 - alarms 252
 - alarms action 246
 - alarms escalation 246
 - cancel 252
 - case management, generate 334
 - components, add an image 291
 - device summary 30
 - device type count 155
 - download 252
 - event time 155
- reports (*continued*)
 - image, add 291
 - include image 291
 - layout 288
 - notifications, add recipients 157
 - out-of-box 285
 - quarterly, set start month 285
 - query ePO devices 150
 - queue 252
 - remove 252
 - show host names 292
 - stop 252
 - user-defined 285
- respond to
 - alarms 250
- restart multiple devices 31
- restore
 - system settings 206
- restore backed up configuration files 208
- restore ELM from back up 104
- restore ESM settings 208
- retention, set up data limits 189
- retrieve rule updates 406
- risk
 - threats to include in calculation 348
- risk correlation engine, ACE 111
- risk correlation manager, add 112
- risk correlation scoring 114
- risk severitythreat management
 - managing 348
 - views, custom and pre-defined 348
- root certificate, upload for CAC 198
- rules
 - add alarm 265
 - add to watchlist 409
 - advanced syslog parser 378
 - check for updates 20
 - clear updates status 407
 - compare files 407
 - copy and paste 402
 - data source 392
 - delete custom 402
 - export 404
 - filter existing 404
 - history, view change 408
 - import 402
 - modify 402
 - modify aggregation settings 410
 - normalization 361
 - override action on downloaded 411
 - retrieve updates 406
 - severity 412
 - transaction tracking, add or edit 397
 - trigger events 117
 - types and properties 361

- rules (*continued*)
 - update credentials [19](#)
 - variables [398](#)
 - view custom [402](#)
 - view signature [406](#)
 - Windows events [400](#)
- rulesets [87](#)
- S**
- SAN storage device, format to store ELM data [99](#)
- scans, run McAfee Vulnerability Manager [151](#)
- scoring, risk correlation [114](#)
- SDEE data sources [81](#)
- search job [107](#)
- search job, create [108](#)
- search job, view results [109](#)
- search, enhanced ELM [307](#)
- secondary Receiver-HA device, reinitialize [46](#)
- security features [194](#)
- security log failure
 - UCAPL, alarm [254](#)
- security, SSH communication keys [24](#)
- selection rule for virtual devices, manage [38](#)
- sensitive data masks [139](#)
 - manage [139](#)
- serial number
 - system [155](#)
 - view device [25](#)
- ServicePortal, finding product documentation [10](#)
- session details, view [297](#)
- session hijacking, TCP [400](#)
- session viewer, display passwords [119](#)
- severity
 - alarms [246](#)
 - alarms escalation [246](#)
 - data sources [75](#)
 - maps [75](#)
 - weights [412](#)
 - weights, set up [412](#)
- shared queries, disable [211](#)
- signature IDs for health monitor [257](#)
- signature, view rules [406](#)
- SMS
 - alarms [239](#)
- SNMP
 - alarms [239](#)
 - configuration [179](#)
 - configure notifications [33](#)
 - MIB [182](#)
 - power failure notification [181](#)
 - settings [179](#)
- SNMP traps
 - UCAPL, alarm [254](#)
- software
 - update on multiple devices [31](#)
- software, update ESM [19](#)
- source events
 - alarms, correlation [241](#)
 - correlation, alarms [241](#)
- source events, view for correlation event [51](#)
- source IP addresses, show host name in report [292](#)
- sources, add data enrichment [221](#)
- SSH
 - communication keys, manage for devices [24](#)
 - communication, disable with ESM [35](#)
 - regenerate key [216](#)
- start devices [35](#)
- start multiple devices [31](#)
- static routes, add [167](#)
- statistics, view for device [29](#)
- status
 - devices, view policy update [401](#)
- status for cases, add [332](#)
- status of device, download data about [29](#)
- STIX indicator types, supported [235](#)
- stop devices [35](#)
- stop multiple devices [31](#)
- storage
 - set up ESM data [187](#)
 - set up ESM VM data [188](#)
- storage allocation, reduce ELM [97](#)
- storage device, add ELM [94](#)
- storage pool, add or edit [95](#)
- storage pool, add storage device to link to [94](#)
- storage pool, move [96](#)
- storage pool, rebuild mirrored [98](#)
- storage usage, view ELM [106](#)
- storage, ELM alternate location [106](#)
- store ELM data, preparing to [91](#)
- store ELM logs [93](#)
- streaming events for Receiver, NSM, ePO [43](#)
- string normalization
 - create file to import [317](#)
 - manage files [316](#)
- subzones
 - add [347](#)
- switch Receiver-HA roles [49](#)
- sync device
 - clocks [176](#)
- sync device with ESM [33](#)
- synchronize system time [175](#)
- syslog
 - alarms [239](#)
- syslog message
 - UCAPL, alarm [254](#)
- syslog relay support [83](#)
- system clock [155](#)
- system log, view [30](#)
- system navigation tree
 - automatic refresh, discontinue [156](#)

system navigation tree (*continued*)organize devices [25](#)

system settings

back up [206](#)restore [206](#)save to redundant ESM [210](#)

system state

UCAPL, alarm [254](#)**T**tagging, ePO [146](#)

tags

add new [409](#)assign ePolicy Orchestrator to IP address [147](#)assign to rules or assets [409](#)category, add new [409](#)custom, delete [409](#)delete custom [409](#)edit existing [409](#)severity [412](#)tail file data source collection method [72](#)task manager [217](#)

TCP

protocol anomalies [400](#)session hijacking [400](#)TCP protocol anomalies for ADM rules [132](#), [377](#)technical support, finding product information [10](#)templates, alarm messages [240](#)term types for ADM rules [127](#), [372](#)

Threat Intelligence Exchange

integration with ESM

execution history [148](#)threat management [348](#)

threats

enable or disable for risk calculation [348](#)view details [348](#)

threshold

alarms condition [246](#)time custom types, add [320](#)time synchronization [175](#)

time zone

format, change [193](#)time, synchronize time [175](#)timeout, console [22](#)track an event [328](#)transaction tracking rule, add or edit [397](#)

trigger frequency

alarms condition [246](#)

triggered alarms

acknowledge [250](#), [251](#)assignee [251](#)cases [251](#)delete [251](#)edit [251](#)triggered alarms (*continued*)filter [251](#)troubleshoot FIPS mode [419](#)

troubleshooting

Receiver-HA failure [50](#)

tuning

alarms [253](#)types of rules [361](#)**U**

UCAPL

administrative roles, alarm [254](#)alarms, create [254](#)audits, alarm [254](#)certificates, alarm [254](#)concurrent sessions, alarm [254](#)failed logons, alarm [254](#)no activity threshold, alarm [254](#)security log failure, alarm [254](#)SNMP traps, alarm [254](#)syslog message, alarm [254](#)system state, alarm [254](#)UCF filters [321](#)

update

software on multiple devices [31](#)status for devices, view policy [401](#)update DEM license [134](#)update ESM software [19](#)updated rule status, clear [407](#)

updates

check for rule [20](#)retrieve rule [406](#)

upgrade

primary and redundant ESM [218](#)

upload

audio files [244](#)

URL link

add device information [27](#)

URL links

add to device [31](#)

user identification

add rule [140](#)manage [140](#)

users

add [192](#)add CAC login [198](#)authenticate to LDAP server [201](#)default name [17](#)disable [201](#)re-enable [201](#)working with [191](#)**V**VA data, integrate [56](#)

- VA data, retrieve [61](#)
- VA retrieval, troubleshoot [62](#)
- VA source, add [58](#)
- VA system profile, define [57](#)
- VA vendors available on ESM [62](#)
- variables [398](#)
 - category, add new [398](#)
 - custom, add [398](#)
 - delete custom [398](#)
 - import [398](#)
 - modify [398](#)
 - modify type [398](#)
- version, view software [25](#)
- view
 - manage queries [217](#)
- views
 - add custom [229](#)
 - change default [316](#)
 - components [308](#)
 - data in a view [298](#)
 - enhanced ELM search [307](#)
 - filtering [298](#)
 - filters [298](#)
 - flow [306](#)
 - host names, display instead of IP address [229](#)
 - manage [297](#)
 - predefined [228](#)
 - query ePO devices [150](#)
- virtual devices [36](#)
 - add to device [38](#)
 - selection rules, manage [38](#)
- virtual local drive [101](#)
- visual alerts
 - alarms action [246](#)
- VLAN
 - add [167](#)
- VM, set up data storage [188](#)
- vulnerability
 - assessment [343](#)
 - manage sources [343](#)

- vulnerability (*continued*)
 - severity [412](#)

W

- watchlist
 - add [301](#)
 - add rules [409](#)
 - create new [408](#)
 - GTI [304](#)
 - manage queries [217](#)
 - overview [301](#)
 - Threat Intelligence Exchange watchlist [148](#)
 - update with alarm data [304](#)
- watchlists
 - Active Response
 - add watchlist [325](#)
 - Active Response search results [325](#)
 - alarms action [246](#)
 - Internet sources [304](#)
- web mail protocol modules for ADM rules [131](#), [376](#)
- weights, set up severity [412](#)
- WHOIS
 - lookup, perform [309](#)
- Windows
 - event ID filters [321](#)
 - events rules [400](#)
- Windows security logs [74](#)
- WMI event log [74](#)
- workflow tracking [328](#)

Z

- zone management [343](#)
- zones
 - add [344](#)
 - add a subzone [347](#)
 - export settings [345](#)
 - import zone settings [345](#)
 - manage [343](#)

