McAfee Enterprise Security Manager 11.0.0 Product Guide

COPYRIGHT

Copyright © 2018 McAfee, LLC

TRADEMARK ATTRIBUTIONS

McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered 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 MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

1 Product overview

Contents

Overview

The McAfee Security Information Event Management (SIEM) solution provides real-time visibility to all activity on your systems, networks, database, and applications.

The solution is composed of the following components:

- McAfee® Enterprise Security Manager (McAfee ESM) - serves as the foundation of McAfee's SIEM solution and provides:
  - Analyst-centric dashboards, reports, views, rules, and alerts
  - Prepackaged configurations (called *content packs*) for common security use cases (such as alarms, views, reports, variables, and watch lists)
  - Predefined dashboards, audit trails, and reports for global regulations and control frameworks
  - Customizable compliance reports, rules, and dashboards
- McAfee® Event Receiver - collects, parses, and normalizes large amounts of raw security data
- McAfee® Enterprise Log Manager (ELM) - provides long-term storage of raw logs for compliance purposes
- McAfee Enterprise Log Search (ELS) - provides quick access to raw logs for forensic purposes
- McAfee® Advanced Correlation Engine (McAfee® ACE) - correlates parsed data to identify trends and suspicious activity
- McAfee® Application Data Monitor (ADM)- monitors unencrypted layer seven session data to identify suspicious activity at the application and protocol level
- McAfee® Database Event Monitor - monitors and tracks database transactions to identify suspicious activity happening in the database communication on the network

Key features

McAfee ESM delivers performance, actionable intelligence, and solution integration at the speed and scale required for security organizations. You can quickly prioritize, investigate, and respond to hidden threats and meet compliance requirements.

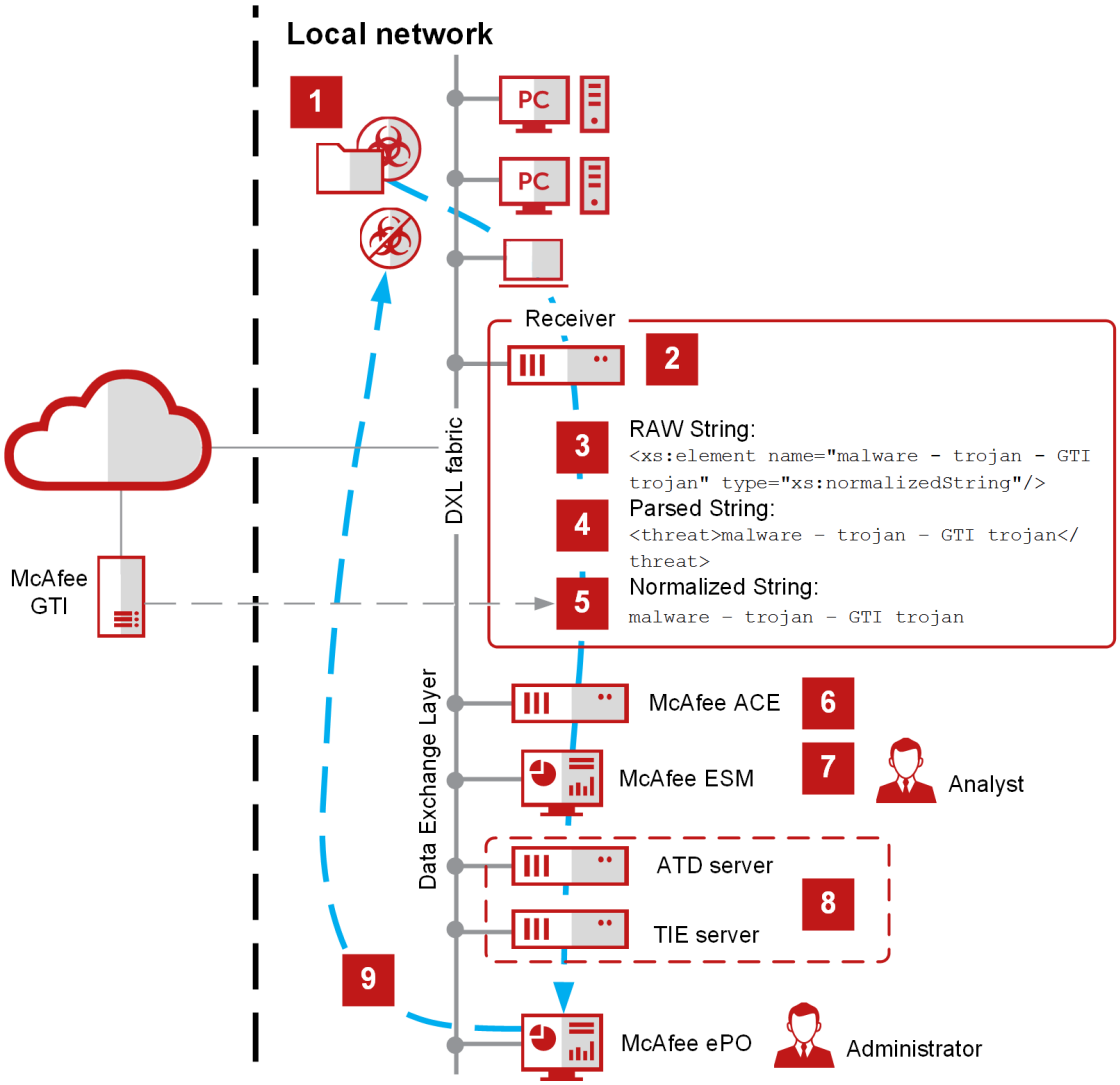
McAfee ESM key features include:

- Analyst-centric dashboards, reports, views, rules, and alerts
- Content Packs with prepackaged configurations (such as rule sets, alarms, triggers, automatic remediation, views, reports, variables, and watch lists) for common security use cases
- Predefined dashboards, audit trails, and reports for global regulations and control frameworks
- Customizable compliance reports, rules, and dashboards
- Ability to enrich events with contextual information (such as privacy solutions; threat data and reputation feeds; and identity and access management systems)
- Near real-time or historical aggregation and correlation of suspicious or confirmed threat information against event data
- Ability to collect data from third-party security vendor devices and threat intelligence feeds
- Rapid access to long-term storage of event data
- Scalable data architecture that collects and correlates log events from multiple years
- On-demand queries, forensics, rules validation, and compliance

How it works

The diagram below shows the McAfee ESM workflow.

1. Threat enters your organization.
2. The McAfee Event Receiver collects data and events from security devices, databases, networks, systems, and applications.
3. The McAfee Event Receiver collects raw data.
4. The McAfee Event Receiver parses (or extracts) data into parts and relationships based on your specific syntax rules.
5. The McAfee Event Receiver normalizes (or aligns) collected values to one common scale and uses to identify known threats.
6. The McAfee Advanced Correlation Engine (McAfee ACE) correlates (or identifies) patterns in the information to identify potential security threats.
7. You, the analyst, can use the McAfee ESM dashboard, alarms, watch lists, cases, and reports to monitor and identify threats.
8. Use the Data Exchange Layer (DXL), McAfee Advanced Threat Defense (ATD), and McAfee® Threat Intelligence Exchange (TIE) to identify threat.
9. Use McAfee ePolicy Orchestrator to respond to threat immediately and automatically.



McAfee ESM Resources

Maximize your McAfee ESM expertise by connecting with these resources.

- McAfee Connect - content pack catalog
- Data Source Configuration Reference
- Support Portal

2 What to do first

Contents

Log on for the first time

After you install and set up devices, you can log on to McAfee ESM 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**.

   When using IPMI, do not use these special characters in your password: `~!@#$%^&*()[]\{}|;':"<>
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, you cannot undo it.
6. Follow the instructions to get your user name and password, which are needed for access to rule updates.

7 Perform initial McAfee ESM configuration:
   a Select the language to be used for system logs.
   b Select the time zone where this McAfee 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.

Customize the logon page

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

Selecting a custom logo has no effect.

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.
   - 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 list.

Change language for event logs

When you first log on to McAfee 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**.

Change the default view

Set the default view that you see when you first log on to McAfee ESM. You can change this default view to any predefined or custom McAfee ESM view.

Task

1 On theMcAfee ESM console, click **Options** | **Views**.

2 On the **Default System View** drop-down list, select the new default view, then click **OK**.

Set console timeout value

Define how long current sessions on the McAfee 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.

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**.

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. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Rules Update**.
4. 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.
5. Click **OK**.

Apply predefined content packs

When a specific threat situation occurs, respond immediately by importing and installing relevant content packs, which contain use-case driven correlation rules, alarms, views, reports, variables, and watchlists to address specific threat activity. Save time by using content packs instead of developing tools in-house.

Before you begin

Verify that you have the following permissions:

- System Management
- User Administration

> If you have customized content pack elements, the update process might overwrite the customized elements.

Task

1. Go to the McAfee Connect Catalog. Browse the available content packs and download the one you want.
2. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
3. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
4. Click **Content Packs**.
5. Click **Browse**.
6. Browse the list and select the content pack you want.

> Clicking a name or description shows the details for that content pack. Clicking the checkbox selects the content pack for installation.

7 Click **Install**.

8 Complete any post-installation steps listed in the details of the content pack.

Connecting McAfee ESM devices

Contents

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.

Manage custom display types

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

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation pane, click the display type drop-down arrow.

3 Do one of the following:

- Click **Add Display**.
- Click the **Edit** icon.

4 Select the settings for the custom display type.

Organize custom display types

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

Before you begin

Make sure that a custom display type has been created.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation pane, click the display type drop-down list and select the custom display.

3 Select the custom display, then do one of the following:

- Click a system or group node, then click the **Add Group** icon. Fill in the fields and click **OK.** Drag-and-drop devices on the display to add them to the group.

  If the device is part of a display tree, the system creates a duplicate device node. You can then delete the duplicate on the System Tree.

- Change properties by selecting the group, then clicking the **Properties** icon.

- Select the group, then click the **Delete Group** icon. The system deletes the group and devices from the custom display but not from the system.

3 Securing McAfee ESM

Contents

How security works

Add users and groups to McAfee ESM, its devices, its policies, and their associated privileges.

When in FIPS mode, McAfee ESM includes **User**, **Power User**, **Key & Certificate Admin**, and **Audit Admin**. When not in FIPS mode, McAfee ESM includes **System Administrator** and **General User**.

McAfee ESM lists:

- **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 the privileges assigned to each group.

Sort the tables by clicking **Username**, **Sessions**, or **Group Name**.

Group privileges

When you set up groups, set privileges that apply to all members of the group.

If you **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 users

Add users to the system so that they have access McAfee ESM, its devices, policies, and associated privileges. Once added, user settings can be edited or removed.

Before you begin

Verify that you have **User Administration** privileges.

Task

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.

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**.

Role (FIPS mode only)	Select a role for this user. The options are:
	• **User** — You cannot add users to a group with **Power User** privileges.
	• **Power User** — These users are system administrators for all Unified Capabilities Approved Products List (UCAPL) purposes, but they might not have all privileges of a system administrator. This role is required for a user to be assigned to a group with any of these privileges:
	  • 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 with **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 with **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 McAfee ESM.

Option	Definition
Email Address	Add the user's email address, which is optional unless the user receives report or alarm notifications. • 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	Add the user's text message (SMS) address. • If the text message (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.

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, and icon indicates whether the account is enabled. If the user has administrator privileges, a different icon appears next to their name.

Define user settings

Define user settings, such as time zone, date format, password, and default display.

Before you begin

If you intend to set specific views for the user, verify that dashboard views exist.

Task

1 On the dashboard, click the user ID drop-down and then click **Options**.

2 Select **User Settings** and select settings for the specific user:

- Select the user's time zone and date format.
- Change the user's password, following the criteria noted.
- Select the default display to appear when the system opens.
- Choose whether to show disabled data sources in the System Tree, the **Alarms** pane, and the **Cases** pane.

3 Select **Views** and select default views for the specific user:

- Choose to refresh views automatically and indicate how often to refresh the view.

  Setting the minimum refresh time to less than 10 minutes for multiple users can impact McAfee ESM performance.

- Select the default system view, Event Summarize view, and Flow Summarize view.

Disable or enable users

Block (disable) or allow (enable) user access temporarily or permanently without deleting them as a McAfee ESM user.

Task

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.

Set up user credentials for McAfee ePO

Set up user credentials to limit access to a McAfee ePO device.

Before you begin

Verify that the McAfee ePO device is set up and does not require global user authentication.

Task

1 On the dashboard, click the user name, then click **Options**.

2 Select **ePO Credentials**.

3 View the McAfee ePO devices on McAfee ESM.

- If the *Not Required* status appears, the device is set up for global user authentication.
- If the *No Credentials* status appears, the device is set up to require individual user authentication.
- To change the user authentication setting, go to the McAfee ePO device **Properties**, click **Connect**, and change the setting in the **Require User Authentication** field.

4 Select a device, then click **Edit**.

5 Type the user name and password, then test the connection.

Set up user groups

Define group settings, such as privileges, policies, and access to devices, reports, and alarm data. Then any user who is part of that group inherits the group settings.

Before you begin

Verify that you have user administration privileges.

Task

1 On the system navigation tree, click **System Properties** | **Users and Groups**, then type your password.

2 Select privileges for this group. Only the item's creator can change permissions for custom items that are read only.

Option	Definition
(Views only) **Inherit permissions from parent folder**	(Default) If you don't want this privilege to be inherited, deselect this option.
(Reports and Watchlists only) **Inherit modify settings**	(Default) Users inherit privileges. Deselect this option if you want to change the default settings.
Groups tab	Indicate the groups with access to the selected items. 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. A pseudo group called *Default* appears for **Master** or **Administrative** users. Groups created in the future get this privilege.
Users tab	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. 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. You can add users to the list or remove them. **1** Click **Add**, click the users, then click **OK**. **2** For each user, select **Read** or **Modify**, then click **OK**. 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.

3 To the right of the **Groups** table, click **Add**, then fill in the information requested on each tab.

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.
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 change.
IP Address Filters	Apply IP address filters to the group to limit data users see when executing reports or selecting users as report or alarm recipients.
Zones	Select zones that users can access and change.
Event Forwarding	Select the event forwarding destinations this group can access. This option defines the devices a user can forward events from and the filters that specify the types of events that can be forwarded. If an event forwarding destination does not belong to an access group, it has access to all devices.
Group Time Restrictions	Limit the days and times this group can access McAfee ESM. Users receive visual notification that their session is going to time out 15, 5, and 1 minute before the time expires.
Reports	Select the reports this group can view and change. You can also select groups or users to share the reports with.
Views	Select the views that users in this group can view and change. You can also share visibility with other users and groups.
Watchlists	Select the watchlists that users in this group can view and change. You can also share visibility with other users and groups.
Filters	Select the filter sets that users in this group can view and change.

If you select more than one view, watchlist, or report, a checkbox in the **Read** or **Modify** column on the **Groups** or **Users** tab indicates a conflict. You can't save and close the page until you resolve the conflict. To resolve the setting for all selected items, click the checkbox.

4 Click **OK**, then type your password again.

Add groups with limited access

To restrict specific users' access to McAfee ESM features, create groups that include 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. All other features are disabled.

Task

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.

Define authentication

Contents

Define logon security

Define logon security settings, such as the number of logon attempts in a specific period, how long the system can be inactive, password settings, and whether to show the last user ID on logon.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **Login Security**.

3 Set the options on the **Standard** tab then click **OK** or **Apply**.

4 Click **OK** or **Apply**.

Option	Definition
Allowed failed login attempts	Specify how many consecutive unsuccessful logons are allowed in a single session. A value of 0 means that infinite logon attempts are allowed. If this number is exceeded in the amount of time specified, the system locks the account. The system administrator must unlock it using the account **Users and Groups**. You cannot lock the master account.
Failed login attempts timeframe	Define the period for successive failed logon attempts (between 0–1440 minutes). This field works with **Allowed Failed Login Attempts**. When the number of allowed failed attempts is reached in a specific period, the system locks the targeted account. It remains locked for the time you set in the **Failed login lockout duration** field or until unlocked by the system administrator.
Failed login lockout duration	Specify the period to lock an account if it auto-locks due to failed logons. Maximum value is 1440 minutes; 0 means you cannot 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. The system always auto-unlocks the master user logon. If you set this period to zero (0), the system temporarily locks the master user logon for five (5) minutes.
UI Timeout Value	Specify the period that must pass without activity before the current session is forced to the logon screen. A value of 0 means there is no limit. For example, if you set this value to 30 minutes, the logon screen automatically appears after 30 minutes of inactivity, forcing the user to log on again to resume activities.
Auto lock inactive accounts after	Set McAfee ESM to lock user accounts without 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 logon.
ACL Settings	Select if you want to set up a list of IP addresses that can access your system or that are blocked from your system.

Define password security

Define security settings for user passwords.

Before you begin

Verify that you have system administrator privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **Login Security**.

3 Click the **Passwords** tab, make your selections, then click **Apply** or **OK**.

Option	Definition
Require advanced password	Identify password requirements, at least: • 15 characters long • 2 numbers • 2 punctuation marks or symbols • 2 lowercase letters • 2 uppercase letters • Cannot include 4 or more consecutive repeating characters The system does not accept passwords that don't meet these requirements.
Password expiration	Specify how often users must change their passwords (0–365 days). If 0 is selected, the password doesn't expire.
Notification prior to password expiration	Select how many days before passwords expire to remind users to change passwords (30-1).
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 in the time period specified after a password expires. After the grace logons, the system locks the account, which can only be unlocked by the administrator.
Password history count	Designate whether to store password history and how many passwords to store for each user (between 0–100 passwords). If set to 0, the system does not store password history. The system checks existing password history when users change passwords. If the password is not unique, the system display an error and does not update the password. If the password is unique, the system changes it and adds a history entry. If the storage limit is reached, the system deletes the oldest password.
Restrict password changes once every	Restrict how often users can change passwords. For example, if you select 12, users cannot change their passwords more than once in 12 hours.

Define RADIUS authentication

Configure McAfee ESM to authenticate users to a RADIUS server.

Before you begin

RADIUS is not FIPS-compliant. If you must comply with FIPS regulations, do not use this RADIUS authentication.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **Login Security**.

3 Select the **RADIUS** tab, then fill in the fields for the primary server, such as IP address, server port, and shared secret (such as password) for your RADIUS server. A secondary server is optional. Then click **OK** or **Apply**.

When you enable the server, all users except the system administrator authenticate with the RADIUS server. If you disable authentication, users set up for RADIUS authentication cannot access McAfee ESM.

Define CAC authentication

Define how to authenticate to McAfee ESM using Common Access Card (CAC) credentials through the browser rather than by entering a user name and password. CAC settings contain client certificates that identify users, similar to the way server certificates identify websites. Before enabling CAC, identify which browsers support CAC and the Electronic Data Interchange Personal Identifier (EDI-PI) associated with CACs.

Before you begin

ActivClient is the only supported CAC middleware on Windows. To use CAC authentication on McAfee ESM from Windows using Internet Explorer, you must install ActivClient on the client computer. Once installed, the system uses ActivClient to manage CAC credentials instead of the native Smart Card manager in Windows. Work with your system administrator to ensure that ActivClient has been installed in your environment.

When relying on CAC validation for application authenticity, the system security depends on the security of the Certificate Authority (CA). If the CA is compromised, CAC-enabled logons are also compromised. To set up CAC logon, upload the CA root certificates, enable CAC logon, 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 McAfee ESM in CAC-enabled browsers without being prompted for a user name or password.

McAfee ESM supports Gemalto and the Oberthur ID One card readers.

Task

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 McAfee 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 McAfee ESM.

2 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

3 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

4 Click **Login Security**, then select the **CAC** tab.

Option	Definition
CAC Mode is currently set to	Select the Common Access Card (CAC) mode. The options are: • **OFF** — This is the default setting. CAC logon is disabled so users have to log on using the McAfee ESM logon prompt. • **OPTIONAL** — CAC authentication is available, but if the user does not provide a certificate, the McAfee ESM logon prompt is shown as if CAC mode were off. • **REQUIRED** — Only CAC-enabled logons can access the system. The logon 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 LCD panel recognizes PIN in IPv4 format (10.0.0.0). Certificates and certificate authorities expire, so **REQUIRED** mode could potentially lock all users out of the McAfee ESM. A fail-safe button is on the LCD panel on the front of the McAfee ESM, which switches CAC mode back to **OPTIONAL**.
Certificate Credentials	Upload the chain of CA root certificates so McAfee ESM has access to them. You can view the certificate file or download it to a location you select.
Certificate Revocation List	Certificate revocation lists (CRL) identify which certificates are revoked. You can manually upload a .zip file with CRL files. 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 McAfee ESM polls for revocation file updates.

5 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.

Define Active Directory authentication

Define how McAfee ESM authenticates users (except the system administrator) with Active Directory. If you disable authentication, users set up for Active Directory authentication can't access the system.

Before you begin

- Set up Active Directory for McAfee ESM.
- Create a group with the same name as the Active Directory group that has access to McAfee ESM. For example, if you name the group *McAfee Users*, you must add a group named *McAfee Users*.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **Login Security**.

3 Click the **Active Directory** tab, then select **Enable Active Directory Authentication**.

4 Click **Add** to set up the Active Directory connection. Then, click **OK**.

Option	Definition
Use as Default	Select if you want to use this domain as the default.
Domain Name	Type the domain name. When logging on to the system, use this domain name as the user name. If you log on using your user name, the system uses the domain designated as the default.
Add button	Add IP addresses used for the Active Directory. • **Administration server** — Select if this is the address for the administration server. If not, deselect it. One of the addresses you enter must identify the host where the administrator server runs. • **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.

Define LDAP authentication

Configure McAfee ESM to authenticate users to an LDAP server.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **Login Security**.

3 Click the **LDAP** tab.

4 Enable LDAP authentication.

When enabled, all users, except the system administrator, must authenticate with the LDAP server. If disabled, users who are set up for LDAP authentication can't access the system.

5 Fill in the fields, then click **Apply** or **OK**.

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.
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.

4 Collecting and processing data

Contents

How data collection works

McAfee Event Receivers enable you to collect and normalize event and flow data into a single manageable view across multiple vendors.

Types of collected data include:

- *Events* - activities recorded by devices as results of your system rules.
- *Flows* - records of connections made between IP addresses, at least one of which is on your HOME_NET.
- *Logs* - event records that occur to your devices.

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 do not indicate anomalous or malicious traffic, they are more common than events.
- Events are associated with rule signature (SigID); flows are not.
- Flows are not associated with event actions, such as alerts, drops, and rejects.
- Flows have unique data, such as source and destination bytes, and source and destination packets.

Source bytes and packets indicate the number of bytes and packets transmitted by the source of the flow. *Destination bytes and packets* indicate the number of bytes and packets transmitted by the destination of the flow.

- Flows have direction: *Inbound flows* originate from outside of the HOME_NET. *Outbound flows* originate from inside the HOME_NET.

Use dashboard views to see events and flows generated by the system. Logs are listed on the **System Log** or **Device Log** accessed from the **Properties** page for the system or each device.

Define data collection settings

Define how McAfee ESM devices collect event, flow, and log data.

Before you begin

Verify that you have the following permissions:

- **Policy Administrator** and **Device Management** or
- **Policy Administrator** and **Custom Rules**

You can select 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 check for each type of information and set inactivity threshold settings for devices managed by McAfee ESM.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the device, then click the **Properties** icon ⚙.

- McAfee Application Data Monitor and McAfee Event Receiver devices collect events, flows, and logs.

  Click **Events**, **Flows & Logs**.

- McAfee ACE and McAfee Database Event Monitor devices collect events and logs.

  Click **Events & Logs**.

- McAfee Enterprise Log Manager and McAfee Enterprise Log Search devices collect logs.

  Click **Logs**.

3 Define the data collection settings (which vary by device), then click **Apply**.

Option	Definition
Auto Update Rules	If McAfee ESM automatically downloads rules from the rules server, select this option to roll out downloaded rules to the selected device.
Auto Download...	Select to check for events, flows, or logs automatically. McAfee Enterprise Log Manager
Get...	Click to check for events, flows, or logs now.
Define daily data pull time range	Schedule a daily time when McAfee ESM pulls data from each device and when each device sends data to the McAfee Enterprise Log Manager. Schedule a time that avoids using the network at peak times, leaving the bandwidth available for other applications. This option can delay data delivery, so determine if this delay is acceptable in your environment. Scheduling event, flow, and log data collection can result in data loss.
Generate Vulnerability Events	Select to add events that match vulnerability assessment source data, become a vulnerability event, and generate an alert on the Local McAfee 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, 20xx at 10:30 a.m. in the **Last Downloaded Event Record** field, click **Apply**, then click **Get Events**, McAfee ESM retrieves events on this device from that time to date.
Inactivity Settings	Define inactivity thresholds for devices so that the system notifies you when those devices don't receive events or flows for the period you specify. If the threshold you set is reached, a yellow health status flag appears next to the device node on the system navigation tree.
Geolocation	*Geolocation* provides the geographic location of computers connected to the Internet. *Autonomous System Number* (ASN) is a number assigned to an autonomous system that uniquely identifies each network on the Internet. McAfee ESM collects source and destination geolocation and ASN data to identify the physical locations of threats. Define whether to store the geolocation and ASN data for each device.

Configure event forwarding

Event forwarding allows you to send events from McAfee ESM to another device or facility via Syslog or SNMP (if enabled). Define the destination, include the packet, and obfuscate the IP address data. You can filter event data before it is forwarded.

The number of event forwarding destinations in use, with the rate and number of events that McAfee ESM retrieves, can affect overall McAfee ESM performance.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Event Forwarding**.
4. On the **Event Forwarding Destinations** page, select **Add**, **Edit**, or **Remove**.
5. If you selected to add or edit a destination, define the settings.
6. Click **Apply** or **OK**.

Set up event forwarding filters

Set up filters to limit the event data forwarded to a syslog or SNMP server on McAfee ESM.

Before you begin

To set up a device filter, verify you have permission to access to the devices in the filter.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Event Forwarding**.
4. Click **Add**, then click **Event Filters**.
5. Fill in the filter fields, then click **OK**.

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.
Severity	To filter by an event severity, select **Greater than or equal** and a severity number between 0 and 100.

Set up event forwarding destinations

Add event forwarding destinations to McAfee ESM to forward event data to a syslog or SNMP server.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Event Forwarding**.

4 Click **Add**, then fill in the requested information.

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 or click **Use System Profile** to add one.
Format	Select the format on the drop-down list. See *Event Forwarding Agents* for a detailed list of the agents and the information contained in 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	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. Unlike UDP, which is a connectionless protocol, a TCP connection must be established between McAfee ESM and the server listening for the forwarded events. If a connection can't be established or is dropped, McAfee ESM tracks the last event successfully forwarded. Then tries to establish the connection again. Once the connection is reestablished, McAfee ESM picks up forwarding event where it left off. If you select UDP, you cannot select SSH or TLS in the **Mode** field.
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 is the same as it was in versions before 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 other parties from examining event forwarding messages. If you are in FIPS mode, you can forward log data using TLS.
Local Relay Port	Type the port to use on McAfee ESM side of the SSH connection.
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 system running the SSH server.

Event forwarding formats

These are the event forwarding formats and the information contained in the packets when they are forwarded.

Format	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, McAfee ESM IP address, CEF version 0, vendor = McAfee, product = McAfee ESM model from /etc/McAfee Nitro/ipsmodel, version = McAfee 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: { "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": "PDE0PjA5MDUyMDE0IDIwOjE4OjQ0fDIxfDY1LjI1NC40OC4yMDAtMzgxMjI8MXwxMDJ8U3BhbSBNZXNzYWdlIHR5cGU6IFRydXN0ZWRTb3VyY2UgU2lnbmF0dXJlIENvbmZpZGVuY2UgPSBISUdILiBDb25uZWN0aW9uOiA2NS4yNTQuNDguMjAwLTM4MTI5KElQLVBvcnQpfFRoaXMgaXMgZGF0YSBm b3IgY3VzdG9tIGZpZWxkIDF8W10A"

Forwarding events with Standard Event Format

Standard Event Format (SEF) is a JavaScript Object Notation (JSON)-based event format to represent generic event data. SEF format forwards events from one McAfee ESM to a receiver on a different McAfee ESM, and from the McAfee 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 one McAfee ESM to another McAfee ESM, complete the following steps:

1. From the McAfee ESM that is forwarding the events, export data sources, custom types, and custom rules.
2. On the McAfee ESM with the receiver you are forwarding events to, import the data sources, custom types, and custom rules that you exported.
3. On the McAfee ESM receiving the events from another McAfee ESM, add an McAfee ESM data source.
4. On the sending McAfee ESM, add the event forwarding destination as follows:
   - From the McAfee ESM dashboard, click ☰ and select **Configuration**.
   - On the system navigation tree, select McAfee ESM, 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 McAfee ESM you are forwarding to, and click **OK**.

Get events and flows

Task

1 On the views toolbar, open the **Refresh** drop-down menu and then select **Get Events and Flows**.

2 In the top table, select the events and/or flows to be retrieved, then click **Start**.

The status of the retrieval is reflected in the **Status** column. The bottom table shows details for the devices selected in the top table.

3 When the download is complete, select a view to display these events and flows in, then click **Refresh** on the views toolbar.

How parsing data works

Contents

How advanced syslog parser works

Advanced Syslog Parser (ASP) parses data from syslog messages based on user-defined rules. Define rules to instruct the ASP how to recognize messages and where event data resides in the messages, such as Signature IDs, IP addresses, ports, user names, and actions.

Use ASP for syslog devices not identified or when the source-specific pParser doesn't correctly interpret messages or fully interpret data points related to received events. You can also use ASP to sort complex log sources, such as Linux and UNIX servers. You must write rules tailored to your Linux or UNIX environment.

Add ASP data sources to the Receiver by selecting Syslog as the vendor. Once you have done this, follow the device manufacturer's directions to configure your syslog device to send syslog data to the IP address for the Receiver.

When you add an ASP source, you must apply a policy before it collects event data. If you enable **Generic Syslog Support**, you can apply a policy without 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.

ASP uses a format similar to Snort.

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

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

Define rules 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	Option of what to do with the event when a match occurs: • 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, filter the effective match based on the protocol.
	Src/Dst IP	If the event defines a source or destination IP address, filter the effective match based on that address.
	Src/Dst Port	If the event defines a source or destination port, filter the effective match based on that port.
Rule Body		The rule body contains most the match criteria and defines how the data must be parsed and logged into the 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 McAfee 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 might 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 McAfee 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 isheld for the use of the setparm keyword. You can change the PCRE keyword by nocase, nomatch, raw and setparm keywords.
	nocase	Causes the PCRE content to be matched whether the case matches or not.
	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 address which is the default source IP address of an event.
* src_port	
* dst_ip	
* dst_port	
* src_mac	
* dst_mac	
* dst_mac	
* genid	This is used to change 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 *Severity and Action Map* 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 *Severity and Action Map* for details.

Tag	Description
* var	This is another way to use setparms. The beneficial use 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. • 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	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: 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" pcre:"PCRE goes here; raw; setparm:firsttime=1; setparm:lasttime=1; adsid:190; rev:1;) For current formats supported, see http://pubs.opengroup.org/onlinepubs/009695399/functions/strptime.html for more detail. %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 %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)

This is an example of a rule that identifies a password based on OpenSSH logon 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 ";pcre:"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;)
```

Mapping syslog severity and action

You can map syslog message severity and action values to values that fit into the system's schema.

- severity_map — Severity displays as a value between 1 (least severe) and 100 (most severe) assigned to events matching the rule. The device sending the message might 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
  ```

  Rule syntax 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
  - 1 = pass
  - 2 = reject
  - 3 = drop
  - 4 = sdrop
  - 5 = alert
  - 6 = default
  - 7 = error
  - 8 = success
  - 9 = failure
  - 10 = emergency
  - 11 = critical
  - 20 = stop
  - 21 = noticed
  - 22 = trusted
  - 23 = untrusted
  - 24 = false positive
  - 25 = alert-reject
  - 26 = alert-drop
  - 27 = alert-sdrop
  - 28 = restart
  - 29 = block
  - 30 = clean
  - 31 = clean-fail

- 12 = warning
- 13 = informational
- 14 = debug
- 15 = health
- 16 = add
- 17 = change
- 18 = remove
- 19 = start
- 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`.

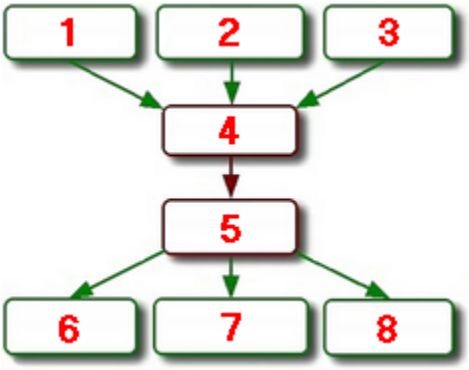
Here is a breakdown of the structure for a rule.

```
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;)
```

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. Sylog-ng and Splunk are supported. This diagram describes this scenario:



1 Cisco ASA Device

2 SourceFire Snort Device

3 TippingPoint Device

4 Syslog Relay

5 Data Source 1 — Syslog Relay

6 Data Source 2 — Cisco ASA

7 Data Source 3 — SourceFire Snort

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.

Upload Syslog Messages 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 [ ].

How Advanced Syslog Parser (ASP) rules work

The Advanced Syslog Parser (ASP) extracts (parses) data out of syslog messages, based on user-defined rules.

ASP 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 the 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 ASP 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 is 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 McAfee 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 McAfee 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.

Optimize your rules by:

- Thoroughly understanding the value that a log can provide to your organization.
- Ensuring that captured values align with the intended use of the specific custom type fields.
- Avoiding indexing fields that contain unique and random or high cardinality data (such as URLs).

- Ensuring that rules mapping event messages directly from the log do not map unique, random, or high cardinality strings as messages. McAfee ESM creates a data source rule for each unique event message, and numerous unique strings can reduce McAfee ESM performance.
- Categorizing 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.

Add custom Advanced Syslog Parser rules

Add custom rules to parse ASP log data.

Before you begin

Verify that you have administrator privileges or belong to an access group with user management privileges.

You must have a working knowledge of Perl-Compatible Regular Expressions.

If you have an advanced knowledge of ASP syntax, you can add ASP rule text directly without defining the settings on each tab.

Task

1 In the **Policy Editor**, select **Receiver** | **Advanced Syslog Parser**.

2 Click **New**, then click **Advanced Syslog Parser Rule**.

3 Select the **General** tab and fill in the information.

Option	Definition
Name	Type a unique, descriptive name for the rule. This text appears in the McAfee 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 McAfee 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 severity value, the system assigns the event 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.

Option	Definition
Process Name	Similar to the content string filter, but only applies to the process name found in the SYSLOG header. Syslog header formats vary widely, so use content strings when possible.
Content String	If a fixed string is always going to be found in the log, add it as a content string. The content strings of an ASP rule should 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 are considered for matching and parsing by the regular expressions. The log must contain all defined content strings. Ensure there is at least one value in the content field section. Content strings should be at least three characters long and be as unique as possible for the specific event. Include enough content matches to uniquely identify the log. Using one or more content fields in the ASP rule can improve the matching and parsing process on the Receiver. 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”.
Regular Expression	The first regular expression determines if the ASP rule matches the log. The system uses additional expressions to capture values from the log.
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 host name 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 side of the Parsing tab as shown below.
Sample Log Data	Paste a sample log entry to be parsed. The system highlights parts of the log that match your regular expressions in blue.

Format	ASP can pre-process certain logging formats to simplify the mapping of data. The following formats are available:
	• 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 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 allow data to be mapped using the JSON key names found in the log
	• XML - Basic, Simple, or Positional - This allows ASP to parse logs that are in XML format and assign parsed data. The XML format choice depends on the type of XML that is in the logs.
	  • 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	The Key/Value fields on the right display what is being parsed from the log samples by the regular expressions. The Key displays 2 numbers, separated by a colon. The first number indicates the regular expression being used, and the second number indicates the capture group used in that regular expression. If a captured value is the fourth capture in the third regular expression defined, the key would display 3:4.
Only use regular expressions for parsing purposes	The parser uses the content string (instead of a regular expression) for matching. Regular expressions are used only to parse messages.

Option	Definition
Case Insensitive	If the log can contain either upper- or lowercase letters in some fields, it might 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.
Trigger when data doesn't match	Triggers the rule when the regular expression does not match the log.

5 Select the **Field Assignment** tab and fill in the information.

a Drag and drop the values from the right side to the **Expression** column next to the **Field** column 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 wanted field, then click **OK**.

6 Select the **Mapping** tab and fill in the information.

Option	Definition
Time Format	The date/timestamp of a log message can be parsed using the variables defined in these fields. McAfee ESM recognizes many standard date/timestamps automatically, but there can be unrecognized formats or ones that display differently. This section allows formatting the time to show up in the proper format when parsed.
Action Mapping	Use this option if there is an action found in the log to be mapped to an available McAfee ESM.
Severity Mapping	The severity mapping allows for a value in 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**, 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**.

Define order for ASP and filter rules

Set the order to run filter or Advanced Syslog Parser (AsP) rules so they generate the data you need.

Before you begin

Verify that you have policy administration privileges.

Task

1 On the McAfee 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.

Rules available to put into order appear on the left; ordered rules appear on the right.

3 On the **Standard Rules** or **Custom Rules** tab, move a rule from the left to the right (drag and drop or use the arrows), placing them above or below **Unordered Rules**.

Unordered Rules represent the rules in the left, which are those that are in default order.

4 Use the arrows to reorder the rules, then click **OK** to save the changes.

Add time formats to Advanced Syslog Parser (ASP) rules

Add custom time formats to Advanced Syslog Parser (ASP) rules so that they can sync up with the time formats of ASP logs.

Task

1 On the dashboard, click the **Policy Editor** icon .

2 In the **Rule Types** pane, select the receiver, then click **Advanced Syslog Parser**.

3 Select a rule, then click **Edit** | **Modify**.

4 Select the **Mapping** tab, then click the plus icon above the **Time Format** table.

5 Click in the **Time Format** field, then select the time format.

6 Select the time fields that you want to use this format.

First Time and **Last Time** see the first and last time the event is generated. Added **Custom Type** time fields also appear.

7 Click **OK**, then complete the remaining information.

Import log samples

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 McAfee ESM dashboard, click ☰ and select **Configuration**.

2 In the navigation tree, select the data source, then click the Properties icon.

3 Click **Upload**.

4 Navigate to the log sample file and select it.

5 Click **Upload**.

6 Click **Close**.

7 Click **Get Events and Flows**.

8 Select **Events** then click **Start**.

9 Find the events in the dashboard and verify the newly created ASP rule is parsing as expected.

How data enrichment works

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 in 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, and run a query. Events that trigger on McAfee ESM are not enriched. Data acquisition takes place on McAfee 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.

Add data enrichment sources

Add a data enrichment source and define which devices receive the data.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **Data Enrichment** | **Add**.

Tabs and fields on the **Data Enrichment Wizard** vary based on the enrichment type you select.

3 On each of the tabs, complete the fields, then click **Next**.

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.

Source tab	• 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 (=).
	For example, a file that uses IP address to host names might look like this:
	`10.5.2.3=New York`
	`10.5.2.4=Houston`	

	Type	Type of database driver for the source.
	Authentication	Default is **None**. If you select **Basic**, enter user name and password for the website if it requires you to log on.

Tab	Option	Definition
	DB Name	Name of the database.
	Host	Name of the computer running the database.
	Ignore Invalid Certificates	If the website 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	(Not required) Apache Hadoop Job Tracker Host address or IP address. If blank, the system uses the Node Name Host.
	Job Tracker Port	(Not required) Port where the Job Tracker Host listens. If blank, the system uses the Node Name Host.
	Method Default setting is **GET**	Default is **GET**. If **POST** is selected, the post content or argument that might be required to navigate to the webpage with the content that you want to search on.
	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	(Not required) Port where the Node Name Host listens. 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`.
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 (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).
	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 `\n`, 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.

Tab	Option	Definition
	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 McAfee 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, or PIG 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.
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.

4 Click **Finish**, then click **Write**.

5 Select the devices you want to enrich and create the field mapping rule for those devices. Then click **OK**.

If you select **Use Static Value**, you must enter the enrichment value.

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

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": " ZW1wbG95ZWVJbmZv",
"qualifier": "dXNlcm5hbWU=",
"latestVersion": true,
"comparator": {
"type": "BinaryComparator",
"value": "c2NhcGVnb2F0"
}
}
</filter>
</Scanner>
```

5 Complete the **Scoring** and **Destination** tabs.

Add Hadoop Pig data enrichment source

Use Apache Pig query results to enrich Hadoop Pig events.

Task

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.

Add Active Directory data enrichment for user names

Use Microsoft Active Directory to populate Windows events with the full user display names.

Before you begin

Verify that you have the System Management privilege.

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.

How normalization works

Rule names can vary by vendors, making it hard to gather event information. McAfee ESM continuously compiles a list of *normalized* rule IDs that enable you to organize event information. Use normalized event IDs to view query results in pie charts, bar charts, and lists or filter dashboard views.

Normalization IDs

Use normalized IDs to:

- Filter using a single ID
- Filter by multiple folders or IDs at one time (using the **Ctrl** or **Shift keys** to select).
- Filter first-level folders

  A mask (/5 for a first-level folder at the end of the ID) means McAfee ESM filters events by the selected subfolder IDs.
- Filter second- or third-level folders

  A mask (/12 for a second-level folder, /18 for a third-level folder at the end of the ID) means McAfee ESM filters events by the selected subfolder IDs.

  The fourth level doesn't have a mask.

String normalization

Use string normalization to:

- Set up a string value that can be associated with alias values
- Import or export a .csv file of string normalization values
- Filter the string and its aliases

For example, for the *John Doe* user name string, define a string normalization file where the primary string is `John Doe` and its aliases are `DoeJohn`, `JDoe`, `john.doe@gmail.com`, and `JohnD`.

You can then enter *John Doe* in the 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 logon inconsistencies where source IP addresses match but user names do not.

How string normalization works

You can normalize strings by associating string values with their corresponding alias values. Then, you can filter queries by strings and import or export the normalized string values.

For example, the *John Doe* user name string, define a string normalization file where the primary string is *John Doe* with the following aliases:

- DoeJohn
- JDoe
- john.doe@gmail.com
- JohnD

You can then create a query with *John Doe* as a user nickname and filter by string normalization.

The resulting view displays all events associated with *John Doe* and his aliases, enabling you to check for logon inconsistencies where source IPs match but user names do not.

Create string normalization files 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

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.

Manage string normalization files

Before you can use a string normalization file, you must add it to McAfee ESM.

Task

1 On the **Filters** pane, click the **Launch string normalization manager** icon .

2 Perform any of the available actions, then click **Close**.

How aggregation works

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 McAfee 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:

- **First time** = 12:00 for the time of the event's first instance
- **Last time** = 12:10 for the time of the event's last instance
- **Total** = 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 McAfee 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.

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** permissions to change these settings.

Event aggregation is available only for ADM devices and receivers, and flow aggregation for receivers.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select the device, then click the **Properties** icon ⚙.
3. Click **Event Aggregation** or **Flow Aggregation**.
4. Define the settings, then click **OK**.

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

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 continue.
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.

Change aggregation settings

Aggregation is set as the default and aggregated events have fields that match. You can choose the type of aggregation for all events generated on a device. Then, you can change the aggregation settings for individual rules.

Task

1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule.

2 Select the rule for which you want to change 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. The descriptions for level 1, level 2, and level 3 aggregation changes based on your selections.

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.

View 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

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the device, then click the **Properties** icon ⚙.

3 Click **Event Aggregation**, then click **View** at the bottom of the screen.

4 Make the needed changes, then click **Close**.

5 Correlating data

Contents

How correlation works

McAfee® Advanced Correlation Engine (McAfee® 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 McAfee ACE alerts you if the asset is threatened. Audit trails and historical replays support forensics, compliance, and rule tuning.

Configure McAfee 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 McAfee ACE discovers new zero-day attacks, it determines whether your organization was exposed to that attack in the past, for *subzero day* threat detection.

McAfee ACE devices supplement the existing event correlation capabilities for McAfee ESM by providing two dedicated correlation engines. Configure each McAfee 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, McAfee 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. McAfee 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. McAfee 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.

  McAfee Event Receivers support network-wide, rule-based correlation. McAfee 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 McAfee ACE device with its own policy, connection, event and log retrieval settings, and risk managers.

Add risk correlation score

You must add conditional statements that assign a score to a targeted field.

Task

1 On the system navigation tree, select **ACE Properties**, then click **Risk Correlation Scoring**.

2 Click **Add**, then fill in the requested information and click **OK**.

Option	Definition
Scoring Enabled	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 wanted 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 is 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 (cannot exceed 100 percent).
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.

Add a risk correlation manager

Add correlation managers to calculate the risk levels for the fields that you designate.

Before you begin

- Make sure that an Event Log Manager (ELM) device exists on McAfee ESM.
- Make sure that storage pools exist on the ELM.
- Make sure zones exist.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the McAfee ACE, then click the **Properties** icon ⚙.

3 Click **Risk Correlation Management**.

4 Click **Add**, then fill in the information requested on each tab.

5 Click **Finish**, then click **Write** to write the managers to the device.

Tab	Option	Definition
Main	**Name**	Manager name
	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. If you select **Use Flow Data**, you must also go to **ACE Properties** | **ACE Configuration** | **Data** and select **Flow Data**.
	Logging, **Storage Pools**	Select **Logging** to save the logs on the Event Log Manager (ELM). Select the storage pool on the ELM where you want the logs saved.
	Zone	If you want the data to be assigned to a zone, select it from the drop-down list.
	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 you set up 60 minutes, the system can use an event that is 59 minutes late.
Fields	**Field**	Select the fields that this manager uses to correlate events (maximum of 5 per manager).
	Percentage	Select the percentage that you want each field to have; the combined percentages must total 100 percent. Risk updates, when below 100 percent critical, report their criticality in terms of what you have defined as *FYI*, *Minor*, *Warning*, *Major*, and *Critical* (see **Thresholds** tab). For example, if your concept of FYI = 50% of the critical value when the risk = 50% of critical, the severity = 20 rather than 50.
	Correlate	Select if you don't want a field to be used to determine uniqueness. Avoid correlating against multiple high cardinality fields due to high memory requirements The number of risk lines generated depends on the number of unique combinations of all correlated fields.
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 for 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.
	Filter Fields Component	Drag and drop the **Match Component** icon onto a logic element, then complete the **Add Filter Field** page. To edit the conditions of a component after adding it to a logic element, click the **Menu** icon for the component and select **Edit**. You can then change the settings.

Add a correlation manager

To use rule or risk correlation, you must add rule or risk correlation managers.

Before you begin

Verify there is a McAfee® Advanced Correlation Engine (McAfee® ACE) device.

Task

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**.
4. Enter the requested information, then click **Finish**.

How historical correlation works

Use historical correlation to correlate past events.

When the system discovers a new vulnerability, check your historical events and logs to determine whether your organization was exploited in the past. Replay historical events using the **Risk Correlation** rule-less correlation engine and the standard rule-based event correlation engine.

Examine historical events against today's threat landscape in these situations:

- Correlation was not set up during the time certain events triggered; correlating those events can reveal valuable information.
- Set up new correlation based on past triggered events and test the new correlation to confirm results.

Be aware of the following when using historical correlation:

- Real-time correlation cannot run until you disable historical correlation.
- Event aggravation skews risk distribution.
- When you move the Risk Manager back to real-time risk correlation, tune the thresholds.

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.

Enable historical correlation

Enable historical correlation, which reviews the events, applies the filters, and packages the events that apply.

Task

1. On the system navigation tree, select **ACE Properties**, the 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**.

View historical correlation events

After running historical correlation, you can view the generated events.

Task

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 McAfee ESM.

2 Close **ACE Properties**.

3 To view the data:

a On the system navigation tree, select the Advanced Correlation Engine (ACE) device on which you just ran historical correlation.

b On the time period drop-down list, select the period you specified when setting up the run.

How correlation rules work

Correlation rules interpret pattern results in the data. Correlation analyzes data and detects patterns in the data flow, generates alerts for these patterns, and inserts alerts into the McAfee Event Receiver alert database.

Correlation rules are separate and distinct from firewalls or standard rules with attributes that specify its behavior. Each McAfee Event Receiver gets a set of correlation rules from an McAfee ESM (deployed correlation rule set), which is composed of zero or more correlation rules set with user-defined parameter values. McAfee ESM includes a base set of correlation rules, which the rule update server updates.

The rules on the rule update server include default values. When you update the base correlation engine rule set, 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.

When you configure a data source, you enable correlation. Only one correlation data source can be configured per McAfee Event Receiver, in a fashion similar to configuring syslog or OPSEC. Once you configure the correlation data source, you can edit the base correlation rule set to create the deployed correlation rule set using the **Correlation Rule Editor**. You can enable or disable each correlation rule and set the value of each rule's user definable parameters. You can also create custom rules and add correlation components to correlation rules.

How correlation data sources work

A correlation data source analyzes McAfee ESM data, detects suspicious patterns, and generates correlation alerts, which are inserted into the receiver alert database. Only one correlation data source can be configured per receiver, similar to configuring syslog or OPSEC.

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

After configuring a correlation data source, you can:

- Roll out the correlation’s default policy
- Edit the base rules in this correlation's default policy

- Add custom rules and components
- Roll out the policy
- Enable or disable each rule
- Set the value of each rule's user-definable parameters

When adding a correlation data source, select **McAfee** as the vendor and **Correlation Engine** as the model.

Enabling the correlation data source allows McAfee ESM to send alerts to the receiver correlation engine.

Set up correlation rules to compare event fields

Set up correlation rules to compare event fields (for example, compare that the source and destination user are the same). You can also set up a rule that ensures that the source IP address and destination IP address are different.

Task

1. On the McAfee 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**, 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**.

   Numeric fields support the following operators: greater than (>), less than (<), greater than or equal to (>=), and less than or equal to (<=).

Example of custom correlation rules

This example shows how a correlation rule generates an alert when McAfee ESM detects 5 unsuccessful logon attempts from a single source on a Windows system, followed by a successful logon, all in 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 (logon tries first, then a successful logon).

5. Click the **Menu** icon , then select **Edit**.
6. Select **Sequence** to indicate that the actions (first, five unsuccessful logon attempts, and second, a successful logon) must occur sequentially, then set the number of times this sequence must occur, which is "1."

7 Set the period 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 for each action. Once the unsuccessful attempts have occurred in five minutes, the system begins to listen for a successful logon from the same IP source in 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 logon attempts against a Windows system).	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: • **Normalization** • **Authentication** • **Login** • **Host Login** • **Multiple failed login attempts against a Windows host** 4 Click **OK** .
Set the number of times the logon failure needs to occur and the period in which they must occur.	1 Drag and drop the **AND** logic element to the **Filter** bar. The **AND** element is used because there are 5 separate attempts that must occur. The element allows you to set the number of times and the length of time that they must occur. 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 logon.	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: • **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**.

Override correlation rule component

If you set a correlation rule to group by a specific field, you can override a component 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 address, you can override a component of the rule to use the destination IP address. This means that all events have the same source IP address except the events that match the overridden component. Those events have the same destination IP address as the source IP address of the other events. Override rule components to look for a single event going from a particular destination followed by another event that originates from that destination.

Task

1. On the McAfee 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**.

Conflicts when importing correlation rules

Exporting correlation rules creates a file with the rule data. But, the file does not include referenced items such as variables, zones, watchlists, custom types, and assets, which this rule might use.

You might encounter import errors if you import a file with referenced rule items that don't exist on the importing system. For example, if rule 1 references variable $abc, and no variable is defined on the importing system that is named $abc, this condition flags the rule as in conflict.

To avoid conflicts, create the needed referenced items (manually or through import where applicable) or change the correlation rule and rule references.

Immediately after the import the system lists which rules are in conflict (flagged with an exclamation point !) or which failed. You can view and change the rule conflict details from this list.

Add parameters to a correlation rule or component

Use parameters to control how correlation rules behave when they execute. Parameters are optional.

Task

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**.

Identify what triggered correlation rules

Identify what caused the rule to trigger and to 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**.

2 Set rules to show details immediately.

   a On the McAfee 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 McAfee 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.

View source events for correlation event

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

Before you begin

Verify that correlation data sources exist on McAfee ESM.

Task

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.

6 Finding threat details

Contents

How the dashboard works

The McAfee ESM *dashboard* is a visual tool that represents data in a form that enables you to find possible threats quickly.

Once you learn what makes up the McAfee ESM dashboard, you can build interactive views to investigate potential threats unique to your organization.

The McAfee ESM dashboard can contain multiple views and interactive tabs that allow you to move between your views quickly. You can use predefined views or build your own unique views with widgets and filters.

1 Populate your McAfee 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.

Description of view components

There are 12 different components you can add to a custom view. You can use them to set up the view to display data in the best format.

Component	Description
Control Dial	Shows the data at a glance. It is dynamic, and can be linked to other components in the console. It updates as you interact with McAfee ESM. Each dial includes a baseline indicator ( ). Gradients around the outer edge of the dial turn red above the baseline indicator. Optionally, the entire dial can change color to represent anomalous behavior: turning yellow when within a certain threshold of a baseline, or red when that threshold is exceeded. The **Rate** option allows you to adjust the rate of the data that you are viewing. For example, if you are looking at **Current Day** and **Total Events** and change the rate to hour, you see the number of events per hour for the given day. This option is disabled if the query you are viewing is already averaged, such as **Average Severity** or **Average Bytes**.
Source and Destination Graph	Displays the overview activity for event or flow IP addresses. The event option allows you to specify IP addresses and view all attacks performed on the specified IP addresses, as well as view all attacks that the specified IP addresses performed on others. The flow option allows you to specify IP addresses and view the IP addresses that have connected to them, as well as view the connections the IP addresses made. This graph includes an open field at the bottom of the component that allows you to view the source and destination events or flows for a specific IP address. Type the address in the field or select one that you used previously, then click the **Refresh** icon .
Pie Chart	Displays the queried information in a pie graph. It is useful when you have fewer categories to view (for example, a protocol or action query).
Table	Displays the query information in several columns. This component is useful to show event and flow data at its finest granularity.
Bar Chart	Displays the queried information in a bar graph, allowing you to compare the size of each result in a given time range.
List	Displays the selected query data in a list format. This component is useful when you want to view a more detailed list of items in a smaller space.
Distribution	Shows a distribution of events and flows over a period of time. You can set intervals to look at specific time slices to shape the data.

Component	Description
Note Area	A blank component that is used for text-based notes. It allows you to write notes that are related to the current view.
Count	Displays the total events, assets, vulnerabilities, or flows queried for a specific view.
Title	Allows you to create a title or heading for your view. It can be placed anywhere on your view.
Geolocation Map	Shows the destination and source location of alerts and flows on a geolocation map. Options on this component allow you to switch between marking city, state, country, and world areas; zoom in and out; and select locations using the **Ctrl** and **Shift** keys.
Filter List	Displays a list of users and groups in your Active Directory. Once the **Filter List** component is added, other components can be bound to it by clicking the down arrow in the **Source User** or **Destination User** filter fields on the **Query Wizard** and selecting **Bind to Active Directory List**. You can also view event and flow data associated with the **Active Directory** by clicking the menu icon.

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.

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.

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 Tab** and then select **Create New View**.

2 Click **Add Widget** and then configure the widget.

a Give your widget a title.

b From the available options, select a query source, which pre-populates the query fields, filters, and sorting values. You can use the defaults or change the values.

ℹ The query source you choose determines which visualization options you can choose for the widget.

c Select the widget's visualization option. Options include: tables, bar charts, pie charts, list charts, gauges, and interactive donut charts.

d Select whether to bind the widget to data in another widget.

3 Click **Create**. Once the widget appears on your dashboard, you can change its size and placement.

4 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**.

5 Click **Save**.

Manage McAfee ESM views

Managing McAfee ESM 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

1 On the McAfee ESM console, click the **Manage Views** icon.

2 Perform any of the available options, then click **OK**.

Option	Definition
List of views	Select views to display on the views list. If the folder is checked, all its subfolders and views are selected. If the folder's checkbox is black, some of its subfolders and views are selected.
Add Folder	To organize your views, create custom folders. You can drag-and-drop views into custom folders.
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. You can drag-and-drop copied views into other folders.
Share	Select the users or groups who can access and change selected views.
Import	Import view files into McAfee ESM.
Export	Export custom views to share them with another McAfee ESM or keep the file as backup. You cannot export read-only views.
Make this my default view	Specify the default view for your view pane.

View event time

View the exact time that events are inserted into the receiver's database.

Before you begin

Verify that you have the following permissions:

- **View Data** to get events and view the event time
- **View Management** to create a view
- **Event Management** to change events

Task

1 On the McAfee 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 Click and drag the **Table** component, then click **Next**.

c 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, 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 at the bottom of the table.
- Click the **Advanced Details** tab, then view the **Device Time** field.

View session details

View event details with a session ID and save them to a csv file on the **Session Viewer**.

To have a session ID, an event must reside in a session. A session is the result of a connection between a source and destination. Events that are internal to the device or McAfee ESM do not have session IDs.

Task

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.

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.

How filters work

In the filters pane, add and delete filter fields, save filter sets, change the default set, manage all filters, and start the string normalization manager. Any filters that are applied to a view are carried forward to the next view that is opened.

When you first log on to McAfee ESM, the default filters pane includes the **Source User**, **Destination User**, **Source IP**, and **Destination IP** filter fields.

An orange funnel icon appears in the upper-right corner of the view pane indicates that filters are applied to the view. Click the orange icon to clear filters and execute the query 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.

How string filters work

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.

Use the *contains* and *regex* filters in any text or string field. The case insensitivity icon Aa next to filter field names denotes text fields. Other fields that allow the *contains* filter do not have that icon.

Syntax and Examples

Syntax for *contains* is `contains(somevalue)` and for *regex* is `regex(someregularexpression)`.

To make the filters case insensitive, click Aa or include the `/i` regular expression notation, as in `regex(/somevalue/i)`. The search results return values that contain `somevalue`, regardless of case.

The NOT ! and or icons apply to *contains* and *regex* values. To show the values in the search results without a value, enter the value and click the ! icon. If you want the results to show one value or another, enter the values and click or.

Example #1 - A simple search

Indexed fields:	`contains(stra),regex(stra)`
Non-indexed fields:	`stra`
Result:	Returns strings 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 strings in the field that contain *admin* or *NGCP*. The regex OR requires the extra set of parentheses 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 statement returns strings in the field that contain a `$`.

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:	`\\`

If you do not use the HEX value or the slash with regex, the *Invalid Regular Expression (ER5-0015)* error can occur.

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, its `nitroguard`, a 3- or 4-digit primary domain, and `com` or `info`. This regex matches the first 2 expressions but not the others. These are examples to show how regex can be used with the feature.

Caveats

- To avoid higher overhead and slower query performance, use `regex` with values with a minimum of 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.
- Familiarity with bloom filters is recommended.

Fields that support `contains` and `regex`

Access_Resource	File_Operation_Succeeded	Referrer
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

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 specify a time frame for the view, click the clock icon on the filter ribbon and then select the time frame. If you want to query archived partitions, use the legacy Flash interface to set a **Custom Time**.

- 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.

Filter by normalized IDs

When you create views or add filters to a view, you can filter the data using normalized IDs.

Task

1 On the McAfee ESM console, do one of the following:
   - To create a view, click **Filters** on the second page of the **Query Wizard**.
   - To add 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.

Filter by Compliance ID

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 McAfee ESMMcAfee ESM.

- You can filter by Compliance ID to select the required compliance or specific subcomponents, or by Windows event IDs.

To...	Do this...
Add UCF filters	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	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.

Filter views

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

1 On the McAfee ESM console, select the view you want to filter.

2 In the **Filter** pane, filter your view in one of the following ways:

- Type the filter information in the appropriate field. For example, to filter the 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.
- 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	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.
View data that matches regular and OR filters	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. The view includes the data that matches the values in the fields not selected **OR**, and matches either of the values in the fields selected **OR**. At least 2 fields must be selected **OR** for this filter to work.
Make the filter values case-insensitive	Click the **Case-insensitive** icon Aa 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 .

McAfee ESM refreshes 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 deselected and the view shows all data.

View streaming events

View a stream of the events generated by McAfee ePO, McAfee® Network Security Manager, Receiver, data source, child data source, or client you select. You can filter the list and select an event to display in a view.

Task

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**.

How custom types work

Use *custom type* fields to filter views and reports, and to create custom rules. You can add, edit, or remove custom types, as well as export and import them.

Export or import custom types

You can export custom types to a specific location. Use caution when importing custom types, as they replace current custom types on the system.

Custom queries

When setting up queries for a view, you can use predefined custom types to filter the queries. If no data exists for a specific custom type, the query returns without results. To avoid results like 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 a custom type.

For example, to include source user data in query results, select **Source User** as a query field. That field acts as a filter and, if the information contains no source user data, the query returns no results. But, if you select User Field 7 (the user field for source user), that field appears as a column in the table of results and doesn't filter the data. If source user data exists, it appears in this column. If no data exists for this field, the User Field 7 column is blank but other columns are populated.

Custom data types

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`

Subtypes can include a maximum of 8 bytes (64 bits) of data. **Space Usage** displays the number of bytes and bits used. When data exceeds the maximum space, this field indicates, in red, that the space has been exceeded, for example: `Space Usage: 9 of 8 bytes, 72 of 64 bits.`

Name/value custom types

If you select the **Name/Value Group** data type, you can add a custom type that includes a specified group of name/value pairs. You can then filter views and queries by these named pairs, and use them in **Internal Event Match** alarms.

Characteristics include:

- Use a regular expression to filter name/value group fields.
- Pairs can be correlated so they are selectable in the **Correlation rule editor**.
- The Advanced Syslog Parser (ASP) collects the values part of the pair.
- The maximum size for name/value custom types is 512 characters, which include the names. Values exceeding 512 characters are cut off when collected. Limit the size and number of names.
- Names must consist of more than 2 characters.
- Name/value custom types can have up to 50 names.
- Each name in the name/value group appears 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:

- Use `contains(<regular expression>)` syntax or type a value into the non-indexed random string or hashed string fields, then filter custom types.
- 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 or a period and asterisk act as a bar (|) 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 bad regular expression errors.
- You can only use a single `regex()` or `contains()` in non-indexed and indexed string, random string, and hashed string custom type filter fields.
- Signature ID field 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.

Search filters include:

- Single values
- 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

Create custom types

Add custom types to use as filters.

Before you begin

Verify that you have administrator privileges or belong to an access group with user management privileges.

If you have administrator privileges, you can view predefined custom types from in McAfee ESM (**System Properties** | **Custom Types**).

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Custom Types**.

4 Click **Add**.

Option	Definition
Name	Type a name for this custom type.
Data Type	Select a data type from the drop-down list. • **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 9 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.
Events Field or **Flows Field**	Select the custom type's slot for each event or flow.
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, you can only filter this custom type with a regular expression.
Description	Type a description of this custom type.

Option	Definition
Specify the number of subtypes	If you select **Long Custom** or **Short Custom** in the **Data Type** field, you can add custom subtypes. • **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 data type for each subtype. If you select **Boolean**, validation ensures that they appear in groups of 8 subtypes. • **Length** column — If you selected **Integer** or **Unsigned Integer** in the **Data Type** column, select the data length 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 the value pairs names in the text field.

5 Click **OK**.

How queries work

McAfee ESM contains predefined queries that gather data for reports or views.

When adding or editing a view or report, define the query settings for each component by selecting the query type, the query, the fields to include, and the filters to use. 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.

Manage queries

McAfee ESM comes with predefined queries that gather data for reports or views. You can edit some of the settings on these queries and you can add and remove custom queries.

Task

1 Do one of the following to access the **Query Wizard**.

To...	Do this...
Add views	1 Click the **Create New View** icon . 2 Drag and drop a component from the **View Editing Toolbar** to the view pane.
Edit views	1 Select the view you want to edit. 2 Click the **Edit Current View** icon . 3 Click the component that you want to edit. 4 Click **Edit Query** in **Properties**.

To...	Do this...
Design new report layouts	1 On **System Properties**, click **Reports**. 2 Click **Add**. 3 In section 5, click **Add**. 4 Drag and drop a component in the report layout section.
Edit report layouts	1 On **System Properties**, click **Reports**. 2 Select the report to edit, then click **Edit**. 3 In section 5, select an existing layout, then click **Edit**. 4 Click the component in the report layout section, then click **Edit Query** in the **Properties** section.

2 On the **Query Wizard**, do one of the following:

To do this...	Do this...
Add queries	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 Change the settings by clicking the buttons.
Edit custom queries	1 Select the custom query that you want to edit, then click **Edit**. 2 Change the settings by clicking the buttons.
Remove custom queries	Select the custom query that you want to remove, then click **Remove**.

3 Click **Finish**.

How comparing values works

Distribution graphs have an option that allows you to overlay another 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, both sets of data continue to display.

Compare graph values

You can compare the data in a distribution graph with a variable you select.

Task

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.

Set up stacked distribution

To see event distribution related to specific fields, set distribution components on views or reports.

When adding components to views or reports, choose how to stack the distribution. When you access the view, you can change the settings, set the interval, and set the chart type and details.

You can't use **Stacking** and **Compare** in the same query.

Task

1. Drag and drop the **Distribution** component on views or reports, then select the query type.

   Stacking is unavailable 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**.
4. Change settings and set interval and chart type by clicking the **Chart Options** icon .

How log search works

Use the log search view to search log data when at least one McAfee Enterprise Log Manager exists 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 McAfee Enterprise Log Manager.

This view provides 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.

During the search, 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.

The system populates these graphs before the search begins and updates the graphs 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.

Search log data quickly

Search uncompressed log data from the McAfee ESM dashboard using McAfee Enterprise Log Search.

Before you begin

Verify that McAfee Enterprise Log Search is configured.

Task

1. On the dashboard, click ☰ and select **ELS Search**.
2. In the **Filter** bar, enter information you want to find, then click 🔍 to begin the search.

   The system ignores the following words:*but, be, with, such, then, for, no, with, not, are, and, their, if, this, on, into, a, or, there, in, that, they, was, is, it, an, the, as, at, these, by, to, of*.
3. Refine your search results:
   - Click **Search Settings** to create an advanced search.
   - Click **Search History** to view and rerun previous searches.
   - Click ↻ to refresh your search results.
   - Click the drop-down arrow, to filter your search results by time or days.
   - To narrow your search further, enter information in the search results and click 🔍

Perform an enhanced ELM search

Search the logs on one or more ELM devices for information that you define.

Task

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.

Define ELM search jobs and integrity checks

To search the Enterprise Log Manager (ELM) for files that match your criteria, define the parameters for the search job. You can also define integrity checks to determine whether files on the Enterprise Log Manager (ELM) have changed since they were originally stored.

Task

1 From the system navigation tree, select the ELM and then click the Properties icon .

2 Select **Data**.

- On the **Search Logs and Files** tab, configure the search parameters.
- On the **Integrity Check** tab, configure the check parameters.

3 Click **Search**.

Running complex searches over long time spans can cause the search process to stop working. Consider breaking these searches into smaller time spans.

Using regex to query ELM data

The Enterprise Log Manager (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 optimizer process for the database runs the regex-to-bloom query. 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.

Running complex searches over long time spans can cause the search process to stop working. Consider breaking searches for long periods into smaller time spans.

Use SFTP to retrieve ELM logs

Configure the Enterprise Log Manager (ELM) to allow SFTP access to retrieve ELM logs.

Before you begin

You must have **ELM SFTP Access** rights.

Task

1 Open an SFTP client such as WinSCP 5.11, Filezilla, CoreFTP LE, or FireFTP.

2 Connect to the ELM using its IP address and the configured SFTP port.

The date indicates when the system inserted the log to the ELM.

The files are presented in two ways: 1) by data source and then data and 2) by date and then data source.

3 Select the logs and transfer them. Specific steps to accomplish this vary based on the SFTP client you are using.

Maximum number of files for SFTP transfers is 20,000.

How McAfee Active Response searches work

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 McAfee Active Response is installed as an extension on McAfee ePO devices added to McAfee ESM, you can use McAfee Active Response to search from the McAfee ESM. The search generates a list of current endpoint data, allowing you to:

- View the list of search results
- Create a watchlist populated with search results
- Append McAfee Active Response search data to an existing watchlist
- Add a data enrichment source populated with search results
- Export search data

Searching with McAfee Active Response uses McAfee® Data Exchange Layer (DXL).

When using McAfee Active Response on McAfee ESM note that:

- High availability (HA) receivers do not support McAfee® Data Exchange Layer (DXL).
- Date formats from a McAfee Active Response search are returned as `2018-11-05T23:10:14.263Z` and not converted to the McAfee ESM date format.
- When you append McAfee Active Response data to a watchlist, the system does not validate the data, which means you might add data to a watchlist that doesn't match its type.

Search using McAfee Active Response

Use McAfee Active Response to search for current endpoint data.

Before you begin

Add a McAfee ePO device with McAfee Active Response to McAfee ESM.

Task

1 Define search settings for the McAfee ePO device.

a From the McAfee ESM dashboard, click ☰ and select **System Properties**.

b On the system navigation tree, select the device, then click the **Properties** icon ⚙.

c Click McAfee ePO **Properties**, then click **Connection**.

d Select **Enable DXL** and specify an **Agent Wake-up Port** (default is 8081).

2 On the McAfee ESM dashboard, select a view with a table widget, such as **Event Analysis**.

3 Click an event, then click ⋮.

4 Select **Actions** | **Execute Active Response Search**, then select a predefined search type.

ℹ Search types are grayed out if the table doesn't have the appropriate fields for the search.

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 the operating system 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.

View McAfee Active Response search results

After running an McAfee Active Response search, there are actions you can take to manage the data that was generated.

Task

1 Run a McAfee Active Response search.

2 Select a row in the results, then click the **Menu** icon ⋮.

Option	Action	Definition
Table		Lists the results of the McAfee Active Response search.
Menu icon	**Create new watchlist from**	Creates a new static watchlist of the values from the column that you select. You can select multiple rows.
	Append to watchlist from	Appends the values from the column that you select to an existing watchlist. You can select multiple rows. ℹ No validation is performed on the data selected from this table.
	Export	Exports data to a .csv file.
	Active Response Search	Performs another McAfee Active Response search on the row that you select on the table. If there are results, the new data replaces the current data.

Add McAfee Active Response data enrichment sources

You can add data enrichment sources to McAfee ESM that are populated with McAfee Active Response search results.

Before you begin

Add a McAfee ePO device with McAfee Active Response to McAfee ESM.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Data Enrichment**, then click **Add**.
4. Complete the requested information on the **Main** tab.
5. On the **Source** tab, select McAfee Active Response in the **Type** field, then fill in the requested information.
6. Complete the information on the remaining tabs, then click **Finish**.

The source is added and the data you specified is enriched with the McAfee Active Response data.

The McAfee Active Response type is not listed if the McAfee ESM fails to pull the McAfee Active Response collectors over DXL.

7 Responding to threats

Contents

How cyber threat works

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.

Supported ICO types

When you add a manual upload cyber threat feed, McAfee 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 IOC that is normalized for McAfee ESM, you receive an error message.

Table 7-1 Indicator types normalized for McAfee 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
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

Table 7-1 Indicator types normalized for McAfee ESM *(continued)*

Indicator type	Watchlist type
URL	URL
User name	Source User, Destination User, User_Nickname
Windows Registry Key	Registry_Key, Registry.Key (Registry subtype)
Windows Registry Value	Registry_Value, Registry.Value (Registry subtype)

Access threat details

Quickly drill down to threat details, file descriptions, and corresponding events for indicators of compromise (IOC) from external data sources, identified by cyber threat feeds.

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 McAfee ESM console, 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

Set up cyber threat feed for domain

To enable a domain feed, you must have two watchlists to hold IP address and domain data.

Before you begin

Verify that you have the following permissions:

- Cyber Threat Management - allows you to set up a cyber threat feed
- Cyber Threat User - allows you to view the data generated by the feed

Task

1. From the McAfee ESM dashboard, click ☰ and select **System Properties**.
2. Select **Cyber threat feeds** | **Add**, then create a feed.

3 On the **Watchlist** tab, click **Create New Watchlist**, and add two watchlists:

- **Name**: CyberThreatIP, **Type**: **IP Address**
- **Name**: CyberThreatDomain, **Type**: **Web_Domain**

4 In the **Indicator Type** field, select **IPv4**, then select CyberThreatIP in the **Watchlist** field.

5 In the next **Indicator Type** field, select **Fully Qualified Domain Name**, then select CyberThreatDomain in the **Watchlist** field.

6 Complete the cyber threat feed setup, then click **Finish**.

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 you to set up a cyber threat feed
- Cyber Threat User - allows you to view the data generated by the feed

Task

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 actions 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.

Errors on manual upload of an IOC STIX XML file

When you add a manual upload cyber threat feed, McAfee 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 7-2 Cyber threat manual upload errors

Error	Description	Troubleshooting

ER328 — Invalid STIX format	The file format is incorrect.	• 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.
		  • Open Standards for Information Society (OASIS) — Organization in charge of STIX standards.
		  • STIX Project — Contains the various STIX data models, schemas, and xsd documents.

ER329 — No supported IOCs found	The uploaded STIX file doesn't contain indicators that are normalized for McAfee ESM.	If a specific indicator needs to be processed, contact Support so that it can be normalized.

How alarms work

Alarms drive actions in response to specific threat events. You can define conditions that trigger alarms and what happens when alarms trigger.

Build alarms

Before you can build and respond to alarms, ensure that your environment contains the following building blocks:

- Alarm message templates
- Message recipient groups
- Mail server connection
- Alarm audio files
- Alarm reports queue
- Visible alarms pane on the dashboard

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.

Monitor and respond to alarms

View, acknowledge, and delete triggered alarms using dashboard views, alarm details, filters, and reports.

- **Viewing triggered alarms** — The Alarms 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 acknowledged alarms from the Alarms pane on the dashboard, but acknowledged alarms remain on the Triggered Alarms view.
- **Deleting triggered alarms** — The system removes triggered alarms 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.

Refine and tune your alarms as you learn what works best for your organization.

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.

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 McAfee 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	• 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 . The system removes acknowledged alarms from the **Alarms** pane but the alarms remain on the **Triggered Alarms** view.
Delete an alarm	• Select the triggered alarm that you want to delete, then click .
Filter the alarms	• Enter the information that you want to use as the filter in the **Filters** pane, then click .
Change the assignee for alarms	1 To display alarm details, click . 2 Select the alarms, then click **Assignee** and select the new assignee.
Create a case for alarms	1 To display alarm details, click . 2 Select the alarms, then click **Create Case** and make the selections you need.

To...	Do this...
View details about an alarm	1 To display alarm details, click . 2 Select the alarm and do one of the following: • To view the event that triggered the selected alarm, click the **Triggering Event** tab. To view a description, double-click the event. If a single event does not meet the alarm conditions, the **Triggering Event** tab might not appear. • 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 McAfee ePO tags assigned to the event.
Edit triggered alarm settings	1 Click the triggered alarm, then click . Select **Edit Alarm**. 2 On the **Alarm Settings** page, make the changes, then click **Finish**.

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 privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon .

3 Click **Alarms**.

4 Click the **Settings** tab.

5 To view the alarm reports waiting to run, click **View**. McAfee ESM runs a maximum of five reports concurrently.

6 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 McAfee ESM, allowing you to cancel any of them.

7 Click **Files** to select whether to download, upload, remove, or refresh any report on the list.

8 Click **Close**.

Building alarms

Contents

- *Set up correlation alarms to include source events*
- *Logic elements*
- *Create UCAPL alarms*
- *Add field match alarms*
- *Customize summary for triggered alarms and cases*
- *Create alarm message templates*
- *Add health monitor event alarms*
- *Health monitor signature IDs*
- *Add alarms to policy rules*
- *Create SNMP traps as alarm actions*
- *Add power failure notification alarms*
- *Add event delta alarms*
- *Manage alarm recipients*
- *Manage alarm audio files*

Enable or disable alarm monitoring

Toggle alarm monitoring on or off for the entire system or for individual alarms. McAfee ESM alarm monitoring is turned on (enabled) by default.

Before you begin

Verify that you have administrator privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 To disable or enable alarm monitoring for the entire system, click the **Settings** tab, then click **Disable** or **Enable**.

ℹ If you disable alarm monitoring, McAfee ESM generates no alarms.

5 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**. McAfee ESM no longer generates this alarm.

6 Click **OK**.

Create alarms

Create an alarm so that it triggers when your defined conditions are met.

Before you begin

Verify that you have administrator privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**, then click **Add**.

4 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.

5 On the **Condition** tab, identify which conditions trigger the alarm.

Condition	Description
Check Rate	Select how often the system checks for this condition.
Deviation	Specify a percentage threshold to check above baseline and a different percentage below baseline. • **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 McAfee ESM triggers the alarm.
Event Rate	• **Event Count** — Enter the number of events that must occur before McAfee 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 McAfee 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 McAfee 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, McAfee ESM includes the values in the aggregated data in the event count, causing a false positive.

Condition	Description
Field Match	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 in 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 in a 10-minute period, McAfee ESM sends a single notice with 5 alarms. 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.
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.
Internal Event Match	• **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. Values with commas must be in a watchlist or in quotes. • **Field** — Select the type of data this alarm monitors. 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.

6 On the **Devices tab**, select which devices this alarm monitors.

7 On the **Actions** tab, identify what happens when the alarm triggers.

Action	Description
Log event	Create an event on the McAfee 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.

Action	Description
Create case	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. If you plan to escalate alarms, do not create cases.
Update watchlist	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. This action requires **Internal Event Match** as the condition type.
Send message	Send email or text messages to the selected recipients. • Click **Add recipient**, then select the message recipients. • Click **Configure** to select the template (for email, text message, SNMP, or syslog messages) and the time zone and date format to use for the message. Using the following characters in alarm names might cause issues when sending text messages: comma (,), quotation marks ("), parenthesis ( ), forward or backward slash (/ \), semicolon (;), question mark (?), at symbol (@), brackets ([ ]), more than and less than signs (< >), and equal sign (=).
Generate reports	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. 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.
Execute remote command	Execute a remote command on any device that accepts SSH connections, except McAfee devices on the McAfee 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. If the alarm condition is **Internal Event Match**, you can track specific events. Click the **Insert variable** icon ☆ and select the variables.
Send to Remedy	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, McAfee 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.
Assign Tag with ePO	Apply McAfee ePolicy Orchestrator tags to the IP addresses that trigger this alarm. Click **Configure** and select the following information: • **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. This action requires **Internal Event Match** as the condition type.

Action	Description
Blacklist	Select which IP addresses to blacklist when an alarm triggers. Click **Configure** and select the following information: • **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. This action requires **Internal Event Match** as the condition type.
Custom alarm summary	Customize the fields that are included in the summary of a **Field Match** or **Internal Event Match** alarm.

8 On the **Escalation** tab, identify how to escalate the alarm when it is unacknowledged in 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.

Copy alarms

Use existing alarms as templates for new alarms, by copying and saving it with a different name.

Before you begin

Verify that you have administrator privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 Select an enabled alarm, then click **Copy**.

The **Alarm Name** page displays the name of the current alarm followed by `_copy`.

You can not copy disabled alarms.

5 Change the name, then click **OK**.

6 To change alarm settings, select the copied alarm and click **Edit**.

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 privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 Click the **Settings** tab, then click **Templates**.

5 On the **Template Management** page, click **Add**, then enter the information requested.

6 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**.

7 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.

Logic elements

When you add a McAfee Application Data Monitor device, 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.
- **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.

Create UCAPL alarms

Create alarms that meet Unified Capabilities Approved Products List (UCAPL) requirements.

Before you begin

- Verify that you have administrator privileges or belong to an access group with alarm management privileges.
- Review the steps to Create alarms on page 100

Task

- Set up the alarm types that apply:

Alarm type	Description
Adjustable threshold for failed logons reached	Trigger alarm when multiple failed logons for the same user reach an adjustable threshold. **1** Create an **Internal Event Match** alarm matching on **Signature ID**. **2** Enter a value of `306-36`.
Threshold for no activity reached	Trigger an alarm when a user account is locked due to reaching the no-activity threshold. **1** Create an **Internal Event Match** alarm matching on **Signature ID**. **2** Enter a value of `306-35`.
Allowed concurrent sessions reached	Trigger an alarm if a user tries to log on to the system after reaching the number of allowed concurrent sessions. **1** Create an **Internal Event Match** alarm matching on **Signature ID**. **2** Enter a value of `306-37`.
Failed system file integrity check	Trigger an alarm when a system file integrity check fails. **1** Create an **Internal Event Match** alarm matching on **Signature ID**. **2** Enter a value of `306-50085`.
Certificates are about to expire	Trigger an alarm when common access card (CAC) or web server certificates are about to expire. **1** Create an **Internal Event Match** alarm matching on **Signature ID**. **2** Enter a value of `306-50081`, `306-50082`, `306-50083`, `306-50084`. The alarm triggers 60 days before the certificate expires, then on a weekly basis. You cannot change the number of days.
SNMP trap sent when system state not approved	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. **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.

Alarm type	Description
Syslog message sent when system state not approved	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. 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	Configure an SNMP trap so that the alarm notifies the appropriate Network Operations Center (NOC) in 30 seconds if a security log fails to record required events. 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**. McAfee ESM sends SNMP traps to the SNMP profile recipient with the message Failed to write to the security log.
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	Trigger an alarm when an administrative session exists for each of the defined administrative roles. 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 field match alarms

Set up alarms to notify you when multiple event fields match and the device receives and parses the event.

Before you begin

- Verify that you have administrator privileges or belong to an access group with alarm management privileges.
- Review how to use logic elements.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 Click **Add**, type the alarm name and select the assignee, then click the **Condition** tab.

5 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 in 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.

6 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).

7 Click the **Actions** and **Escalation** tabs to define the settings.

8 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**.

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 privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**, then click **Add** or **Edit**.

4 On the **Condition** tab, select the **Field Match** or **Internal Event Match** type.

5 Click the **Actions** tab, **Create case**, then **Configure**. Then select the fields to include in the case summary.

6 Click **Customize triggered alarm summary**, click ☆, then select the fields to include in the summary for the triggered alarm.

7 Type the information requested to create alarms, then click **Finish**.

Create alarm message templates

Create alarm message templates for email, Short Message Services (text message), 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 privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 Click the **Settings** tab, then click **Templates**.

- To create custom templates, click **Add**.
- To change a custom template, select it and click **Edit**.

  ℹ You cannot edit predefined templates.

- To delete a custom template, select it and click **Remove**.

  ℹ 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**.

5 Click **Add**.

6 On the **Add Template** page, then configure the template.

Option	Description
Type	Select whether this template is for an email or text message. ℹ Text messages (limited to 140 characters) are sent as email to phones then converted to text messages by the carrier.
Name	Type the name for this template.
Description	Type a description of what this template includes.
Make Default	Use the current template as the default when sending messages.

Option	Description
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	Select the fields that you want to include in the body of the message. For syslog message templates, limit the message body to fewer than 950 bytes. McAfee ESM cannot send any syslog message that exceeds 950 bytes. • 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**, McAfee 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. McAfee ESM then includes this information in the message for up to 10 records. • Set up correlation alarms to include source events on page 105 To include source events in alarms that use a correlation event as a match ( ), click the **Insert Field** icon and select **Source Events Block**. When you select **Internal Event Match** or **Field Match** as the alarm type, McAfee ESM includes event field data in the email. Select **Field Match** for data source-driven alarms, which run on the Receiver not McAfee ESM. Select **Internal Event Match** alarms, which run on McAfee ESM and force a query to run every time the alarm frequency expires.

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 privileges or belong to an access group with alarm management privileges.
- Review available Health monitor signature IDs on page 112.
- Review the steps to Create alarms on page 100.

Task

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 (Local ESM). Then select a view that displays the health monitor event (**Event Analysis** or **Default Summary**).

   b Click the event, then click .

c Select **Actions** | **Create new alarm from**, then click **Signature ID**.

d Fill out the remaining settings for the alarm.

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	McAfee 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	McAfee ESM	Medium
Account disabled due to max logon failures	306-36	User account disabled, due to maximum logon failures.	Software Monitor	McAfee ESM	High
Add/Edit Remote Command	306-60	Alarm remote command added or deleted.	Software Monitor	McAfee 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	McAfee ESM	Low
Archive configuration change	306-3	McAfee ESM archival settings changed.	Software Monitor	McAfee 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	McAfee ESM	Low
Audit administrator user logon	306-38	UCAPL event, audit administrator logon.	Software Monitor	McAfee ESM	Low
Backup configuration change	306-1	McAfee ESM backup configuration settings changed.	Software Monitor	McAfee ESM	Low
Backup performed	306-2	Backup performed on the system.	Software Monitor	McAfee 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	McAfee ESM CAC certificate expired.	Software Monitor	McAfee ESM	High
CAC cert expires soon	306-50081	McAfee ESM CAC certificate expires soon.	Software Monitor	McAfee ESM	Medium
Case changed	306-70	Case changed.	Software Monitor	McAfee ESM	Low

Rule name	Signature ID	Description	Type	Device	Severity
Case status added/ modified/deleted	306-73	Case status changed.	Software Monitor	McAfee ESM	Low
Communication channel state change alert	306-50013	Control channel stopped or started.	Software Monitor	All	Medium
Configuration capture failed (device error)	146-4	Network discovery device error.	Software Monitor	McAfee ESM	Low
Configuration capture failed (device unreachable)	146-3	Network discovery device unreachable.	Software Monitor	McAfee ESM	Low
Configuration captured	146-5	Network discovery configuration checked successfully.	Software Monitor	McAfee ESM	Low
Configuration policy failure	146-8	Not used in system.	Software Monitor	McAfee ESM	Low
Configuration policy pass	146-9	Not used in system.	Software Monitor	McAfee ESM	Low
Data allocation configuration change	306-7	McAfee ESM data allocation settings changed.	Software Monitor	McAfee 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	McAfee ESM data retention configuration changed.	Software Monitor	McAfee 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	McAfee ESM	Low
Deleted events	306-74	User deleted McAfee ESM events.	Software Monitor	McAfee ESM	Low
Deleted flows	306-75	User deleted McAfee ESM flows.	Software Monitor	McAfee ESM	Low
Device add	306-18	New device added to the system.	Software Monitor	McAfee ESM	Low
Device delete	306-19	Existing device deleted from the system.	Software Monitor	McAfee ESM	Low
Device possibly down	146-2	Network discovery event stating a device can be down.	Software Monitor	McAfee ESM	Low
Device unreachable	146-1	Network discovery device added to McAfee ESM is unreachable.	Software Monitor	McAfee 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	McAfee 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
McAfee ESM reboot	306-32	McAfee ESM rebooted.	Software Monitor	McAfee ESM	Medium
McAfee ESM shutdown	306-33	McAfee ESM shut down.	Software Monitor	McAfee 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	McAfee 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	McAfee ESM	High
Failed to format SAN device	306-50057	SAN on ELM failed to format; user must retry.	Hardware Monitor	McAfee ESM	High
Failed user logon	306-31	User failed to log on.	Software Monitor	McAfee 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	McAfee 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	McAfee ESM failed to obtain VA data.	Software Monitor	McAfee ESM	Medium
Get VA data success	306-51	McAfee ESM obtained VA data.	Software Monitor	McAfee 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	McAfee ESM indexing settings changed.	Software Monitor	McAfee 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 logon	306-39	UCAPL event, Crypto administrator logon.	Software Monitor	McAfee 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	McAfee ESM cannot communicate with another device.	Software Monitor	McAfee 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	McAfee 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	McAfee 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	McAfee ESM	Low
NSM delete Blacklist	306-30	NSM Blacklist entry deleted.	Software Monitor	McAfee 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	McAfee ESM	Low
Policy delete	306-17	Policy deleted from the system.	Software Monitor	McAfee ESM	Low
Policy change	306-16	Policy changed in the system.	Software Monitor	McAfee ESM	Low
Previous configuration mismatch	146-6	Network discovery device configuration changed.	Software Monitor	McAfee 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
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	McAfee 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	McAfee ESM	Low
Rule delete	306-22	Rule deleted from the system.	Software Monitor	McAfee ESM	Low
Rule change	306-21	Rule changed in the system.	Software Monitor	McAfee ESM	Low
Rule update failure	306-9	McAfee ESM rule update failed.	Software Monitor	McAfee ESM	Medium
SDEE retriever state change alert	306-50033	SDEE collector stopped or started.	Software Monitor	Receiver	Medium
sFlow collector state change alert	306-50025	sFlow (flow) collector stopped or started.	Software Monitor	Receiver	Medium

Rule name	Signature ID	Description	Type	Device	Severity
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	McAfee 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	McAfee 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	McAfee ESM	Low
User device failed logon	306-50079	SSH user failed to log on.	Software Monitor	McAfee ESM	Low
User device logon	306-50017	Not used in system.	Software Monitor	McAfee ESM	Low
User device logout	306-50078	SSH user logged out.	Software Monitor	McAfee ESM	Low
User logon	306-11	User logged on to the system.	Software Monitor	McAfee ESM	Low
User logout	306-12	User logged out of the system.	Software Monitor	McAfee 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	McAfee ESM	Low
Variable delete	306-25	Policy variable deleted.	Software Monitor	McAfee ESM	Low
Variable change	306-24	Policy variable changed.	Software Monitor	McAfee ESM	Low
Web Server cert has expired	306-50084	ESM web server certificate expired.	Software Monitor	McAfee ESM	High
Web Server cert will expire soon	306-50083	ESM web server certificate expires soon.	Software Monitor	McAfee ESM	Medium
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

Add alarms to policy rules

Set up policy rules with alarms that notify you when the rules generate events.

Before you begin

Verify that you have administrator privileges or belong to an access group with alarm management privileges.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree toolbar, click the **Policy Editor** icon .
3. Select the type of rule in the **Rule Types** pane.
4. Select one or more rules in the rules display area.
5. Click and create an alarm.

Create SNMP traps as alarm actions

Send SNMP traps as an alarm action.

Before you begin

- Verify that you have administrator privileges 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).

Task

1. Create an SNMP profile to tell McAfee ESM where to send the SNMP traps.
   a. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
   b. On the system navigation tree, select McAfee ESM, then click the **Properties** icon .
   c. Click **Profile Management**, then click **Add**.
   d. Select **SNMP Trap** as the **Profile Type**.
   e. Fill in the remaining fields, then click **Apply**.
2. Configure SNMP on McAfee ESM.
   a. On **System Properties** | **SNMP Configuration**, 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** | **Alarms**, 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** | **Configure** to select or create a template for SNMP messages.

d Select **Basic SNMP Templates** in the **SNMP** field, or click **Templates**. Then 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 power failure notification alarms

Alarms can notify you when McAfee ESM power supplies fail.

Before you begin

- Verify that you have administrator privileges or belong to an access group with alarm management privileges.
- Set up SNMP trap for power failure notification on page 202

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 Click **Add**, enter the requested data on the **Summary** tab, then click the **Condition** tab.

5 In the **Type** field, select **Internal Event Match**.

6 In the **Field** field, select **Signature ID**, then type `306-50086` in the **Value(s)** field.

7 Enter the remaining information as needed for each tab, then click **Finish**.

An alarm triggers when a power supply fails.

Add event delta alarms

Out-of-sync data sources can generate events with timing issues. Set up event delta alarms to notify you of possible event timing issues.

Before you begin

Possible event timing issues can occur for several reasons:

- Incorrect time zones are set for McAfee ESM or data sources.
- McAfee ESM has been on for a long time and the timing slips out of sync.
- McAfee ESM isn't connected to the Internet.
- Events are out of sync when it comes into the receiver.

Verify that you have administrator privileges or belong to an access group with alarm management privileges.

When out-of-sync data sources generate events, a red flag appears next to its receiver on the system navigation tree.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Set up alarms when out-of-sync data sources generate events:

   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.

   c Select how often McAfee ESM checks for out-of-sync data sources.

   d Select the time difference that must exist for the alarm to trigger.

   e Complete the information in the remaining tabs.

4 View, edit, or export the out-of-sync data sources:

   a On the system navigation tree, click the receiver, then click the **Properties** icon.

   b Click **Receiver Management** | **Time Delta**.

Manage alarm recipients

Identify alarm message recipients and configure how to send those alarm messages, using email, Short Message Services (text message), Simple Network Management Protocol (SNMP), or syslog.

Before you begin

- Verify that you have administrator privileges or belong to an access group with alarm management privileges.
- Verify that the profiles you intend to use exist.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 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 text message 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 in 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 McAfee 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. • **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. • 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, McAfee ESM begins incrementing from the last OID specified in the list.

5 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.

Manage alarm audio files

Upload and download audio files to use with alarm alerts.

Before you begin

Verify that you have administrator privileges or belong to an access group with alarm management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Alarms**.

4 Select the **Settings** tab, then click **Audio**.

5 Download, upload, remove, or play audio files.

ℹ McAfee ESM includes three pre-installed sound files. You can upload custom audio files.

How watchlists work

Use *watchlists* to filter information or as an alarm condition.

Watchlists can be global or shared to a specific user or group.

Static watchlists contain imported values or values that you enter.

Dynamic watchlists contain values resulting from regular expressions or defined string search criteria.

Watchlists can include a maximum of 1,000,000 values, but McAfee ESM can only display 25,000 values. If more values exist, McAfee ESM notifies you that there are too many values to display.

To add more than 25,000 values to a watchlist, first export the existing list to a local file, add the new values, then import the new list.

If you set up static watchlist with values that expire, the system time stamps each value, which then expires when the specified duration is reached, unless it refreshes. Values refresh if an alarm triggers and adds them to the watchlist. You can also refresh values set to expire by appending them to the list on a view.

For dynamic watchlists, you can set values to update periodically. The system queries the source using the data given and refreshes the values at the specified time.

View IP address event details

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 IP addresses are returned, including risk severity and geolocation data.

Before you begin

Verify that you have a current McAfee GTI license.

Task

1 On the McAfee ESM console, select a view that includes a table component such as **Event Views** | **Event Analysis**.

2 Click an IP address, click ⋮ on any component that has an IP address, then click **IP Address Details**.

McAfee GTI watchlists

McAfee® Global Threat Intelligence™ (McAfee GTI) watchlists contain more than 130 million suspicious and malicious IP addresses and their severities, gathered by McAfee. Use these watchlists to trigger alarms, filter data in reports and views (as a filter in rule correlation), and as a scoring source for a risk correlation manager on a McAfee ACE device.

To populate **GTI Malicious IPs** and **GTI Suspicious IPs** in watchlists, you must purchase a license for McAfee® Global Threat Intelligence™ (McAfee GTI). Then, downloading rules adds the McAfee GTI lists to your system.

Downloading the lists requires an Internet connection (they cannot be downloaded offline). Downloading can take several hours due to the size of the database.

McAfee GTI lists cannot be viewed or edited, but they indicate whether the list is *active* (contains values) or *inactive* (does not contain values).

Share watchlists, reports, and views

Assign privileges to users and groups to see or change views, watchlists, or reports.

Task

1 Open the **Permissions** page for watchlists, reports, or views.

- From the System Properties page, click **Watchlists**, select a watchlist, then click **Share**.
- From the System Properties page, click **Reports**, select a report, then click **Share**.
- From the console, click the **Manage Views** icon, select a view, then click **Share**.

2 Select whether to inherit the settings.

3 If the settings aren't inherited, select which groups or users can view or change the selected items.

When you select **Modify**, the system selects **Read** automatically.

Add watchlists

Use watchlists as filters or alarm conditions.

Before you begin

To populate **GTI Malicious IPs** and **GTI Suspicious IPs** in a watchlist, you must purchase a license for McAfee GTI.

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**.

2 Click **Add** or **Add New Watchlist**.

Tab	Option	Definition
Main	**Name**	Type a name for the watchlist.
	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.	
	ESM Strings	Searches the *StringMap* 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`, such as `/Exploit/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`, such as `/Exploit/i`.

Tab	Option	Definition
	HTTP/HTTPS	Fill in these fields: • **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**.
	McAfee Active Response	Fill in these fields: • **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 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 5 filters.
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 (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).
	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 `\n`, 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**	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, McAfee 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. 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.

Tab	Option	Definition

	Values	For a static watchlist, import a file of values in new-line-separated format or type the values, one value per line.
		
		Both static and dynamic watchlists are limited to a maximum number of 1,000,000 values.
		
		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.
		
		User name identifies who can access the database. For LDAP, the user name must be a fully qualified domain name without spaces, such as:
		
		`uid=bob,ou=Users,dc=example,dc=com`
		
		or
		
		`administrator@company.com`

	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.

3 Click **OK** to add the new watchlist to the **Watchlists** table.

Create rule watchlists

Use *watchlists* to group rules that you can use as filters or alarm conditions that notify you when the rule occurs in an event. These watchlists can be global or specific to McAfee ESM users or groups.

Task

1 In the **Rule Types** pane of the **Policy Editor**, select the rule type, then select the rules that you want to have on this watchlist.

2 Click **Operations**, then select the **Create new watchlist** option.

3 Type a name, then make sure the **Static** option is selected.

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, do one the following:

- 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 a generated event contains any of the values on this watchlist, click **Create Alarm**.

7 Click **OK**.

Add rules to watchlists

After creating watchlists, you can add rule values to it, using the **Append to watchlist** option.

Task

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**.

Create IOC threat watchlists

Create watchlists to pull threat or Indicator of Compromise (IOC) feeds from the Internet. You can preview the data through the HTTP request, and filter the data using regular expressions.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Watchlists**, then click **Add**.
4. Complete the **Main** tab, selecting **Dynamic**.
5. Click the **Source** tab, select **HTTP/HTTPS** in the **Type** field.
6. Complete the information requested on the **Source**, **Parsing**, and **Values** tabs.

The first 200 lines of the html source code populate the **Raw data** field on the **Parsing** tab. It is just a preview of the website, but is enough for you to write a regular expression on which 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 `(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})` to match on an IP address.

Add Hadoop HBase watchlists

Add watchlists using Hadoop HBase as the source.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Watchlists**, then click **Add**.
4. On the **Main** tab, select **Dynamic** and enter the information requested.
5. On the **Source** tab, select **Hadoop HBase (REST)** in the **Types** field. Then type the host name, port, and name of the table.

6 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>
```

7 Click the **Values** tab, select the value type, then click the **Run Now** button.

Create McAfee Active Response watchlists

Set up dynamic watchlists populated with McAfee Active Response search results.

Before you begin

Add a McAfee ePO device with McAfee Active Response to McAfee ESM.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Watchlists**, then click **Add**.

4 Complete the **Main** tab, selecting **Dynamic**.

5 On the **Source** tab, select McAfee Active Response in the **Type** field, then fill in the requested information.

6 Complete the information on the remaining tabs, then click **Finish**.

The watchlist is added and collects the data you specified from McAfee Active Response searches.

The McAfee Active Response type is not listed if McAfee ESM fails to pull the McAfee Active Response collectors over DXL.

How a global blacklist works

A *blacklist* blocks traffic as it flows through a network device before the deep packet inspection engine analyzes it. A *global blacklist* applies to all network devices managed by McAfee ESM.

You can set up a blacklist for individual network devices on McAfee ESM. A global blacklist only allows permanent blacklist entries. To set up temporary entries, 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** allows you to:

- **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. You can add critical IP addresses (for example, DNS and other servers or system administrators' workstations) to the exclusions, ensuring that they are never automatically blacklisted regardless of the events they might generate.

You can configure entries in both **Blocked Sources** and **Blocked Destinations** to narrow the effect of the blacklist to a specific destination port.

When adding entries:

- You can configure blocked source and destination entries to blacklist on all ports, or a specific port.
- Configure entries with a masked range of IP addresses with the port set to any (0) and the duration must be permanent.
- After typing an IP address or host name, 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 use 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 websites.

Set up a global blacklist

Set up a global blacklist to block specific traffic from all network devices that support blacklisting.

Task

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.
   - For **Exclusions**, manage the list of IP addresses that should never be blacklisted automatically, such as DNS and other servers, or the system administrator's workstation.
   - Default is zero (0), which allows any port. Type a port number if you want to narrow the effect of the blacklist to a specific destination port.
3. Select the network devices that support the global blacklist.

Add blacklist entries for McAfee Network Security Manager

McAfee Network Security Manager applies blacklisting through the sensors.

Before you begin

You must be a super user to use the blacklist function.

Task

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**.

If duplicate IP addresses exist, the global blacklist address overwrites the McAfee Network Security Manager address.

Once you select this option, you can only delete items manually.

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

The entry appears on the blacklist until its duration expires.

Manage removed blacklist entries for McAfee Network Security Manager

Entries initiated on McAfee ESM that have not yet expired, but do not return blacklist entries you query McAfee Network Security Manager, display with a **Removed** status and a flag icon.

This condition occurs if you remove the entry, but do not initiate the removal on McAfee ESM. You can add this entry to or delete it from the blacklist.

Task

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**.

How cases work

Use cases to track the work to investigate potential threats.

In dashboard views, create cases based on events that you want to investigate.

You can add contextual details and events to the case notes and track the investigative work. When resolved, close the case and build alarms that apply the information uncovered in this case.

Add cases

Track actions taken in response to events.

Before you begin

Make sure that you have administrator privileges or belong to an access group with case management privileges.

Task

1 Create a new case using Case Management or a context menu.

- From the dashboard, click ☰, click Case Management, then click the **Add Case** icon.
- From the dashboard, select an event, click the menu icon ⋮, then click **Actions** | **Create a new case**.

A summary of open cases appears on the left side of the dashboard.

2 Fill in the information requested, then click **OK**.

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**.

Change cases

You can change case details or close cases. Changes are recorded in the case notes. Closed cases no longer appear on the **Cases** pane, but do display on the **Case Management** list with a *Closed* status.

Before you begin

Make sure you have one of the following case privileges:

- **Case Management Administrator** to change any case on the system.
- **Case Management User** to change only cases assigned to you.

Task

1 From the dashboard, click ☰, then select **Case Management**.

2 Access **Case Details** in one of these ways:

- To select a cased assigned to you, select it on the **Cases** pane, then click the **Edit Case** icon .
- To select a case not assigned to you, click the **Open Case Management** icon and select relevant case. Then, the **Edit Case** icon .

3 You can change cases as follows:

- 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**.
- To set a default case status, click **Add** or **Edit** then click **Default** and choose the default status.
- Select cases you want to appear in the **Cases** pane on the dashboard.

4 Click **OK** to save the changes.

View cases

Manage all cases, whether they are currently open or closed.

Before you begin

Verify that you have administrator privileges or belong to an access group with case management privilege.

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 in Case Management**.

The **Case Details** view opens, listing all cases in the system.

3 Review the data.

Option	Definition
Summary	Summarizes the case (up to 255 characters).
Case ID	Lists unique, system-generated number (you cannot change) given to the case once it has been added.
Assignee	Lists the users or groups to which the case is assigned. Lists all users and user groups who have case management rights.
take	Allows you to reassign the case to yourself.
Severity	Lists case severity: 1–20 = Green 21–40 = Blue 41–60 = Yellow 61–80 = Brown 81–100 = Red
Organization	(Optional) Lists the organization to which the case is assigned. You can add an organization by clicking **Organization**, then clicking **Add.**
Status	Lists current case status; predefined statuses include:**Open** (default) and **Closed**. You can add statuses.
Created	Lists date case created
Last Updated	Lists date case changed

Option	Definition

Notes	Tracks actions taken, which includes the type of action taken or change made, the date and time, and the name of the user.
	For changes, both old and new values are recorded. For example:
	`---- Severity Changed on 04-22-2009 at 09:39`
	`old: Low`
	`new: High`
	The following actions are recorded automatically:
	• Case opened
	• Case closed
	• Changes to the summary
	• Case is reassigned
	• Severity is changed
	• Organization is changed
	• Events are changed

History	Lists users who have accessed the case
Message table	Lists events 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.

Email cases

Set up the system to send an email message automatically to the case assignee, every time a case is added or reassigned. You can also email a case notification manually, and include case notes and event details.

Before you begin

- Verify you have **Case Management Administrator** privileges.
- Set up email addresses for the users on the McAfee ESM.

Task

1 Email a case automatically.

   a On the **Cases** pane, click .

   b Click .

   c Select **Send an email when a case is assigned**, then click **Close**.

2 Email a case manually.

   a On the **Cases** pane, select the case you want to email, then click .

   b On **Case Details**, click **Email Case**, then fill in the **From** and **To** fields.

   c Select whether you want to include the notes and attach a CSV file of the event details.

   d Type any notes you want to include in the email message, then click **Send**.

Generate case management reports

McAfee ESM provides 6 standard case management reports.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Reports** | **Add**.
4. Complete sections 1, 2, and 3.
5. In section 4, select **Query CSV**.
6. 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 and 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 and 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.
7. Complete section 6, then click **Save**.

The selected reports appear on the **Reports** list.

8 Backing up and restoring

Contents

How backup and restore work

You can back up McAfee ESM configuration settings, automatically or manually. Then, if you encounter a system failure or data loss, you can restore your McAfee ESM configuration.

A *standard backup* saves all configuration settings, including those for policy, SSH, Network, and SNMP files. When you add devices, the system automatically enables backup and restore to occur every 7 days.

An *incremental* backup stores compressed McAfee ESM configuration files to either a local or remote storage location. You can set up an incremental backup of events, flows, and logs for the last 24 hours (since the last backup time stamp).

To restore the system, select backup files on McAfee ESM, a local computer, or a remote location to revert settings to a previous state. Changes made to the settings after the backup are lost.

For example, if you perform a daily backup and want to restore settings from the last three days, select the last three backup files. The system adds events, flows, and logs from the three backup files to the events, flows, and logs currently on McAfee ESM. The system then overwrites all settings with the settings in the most recent backup.

Maintain files

Ensure that your backups, software updates, and alarm and report logs are current by maintaining their corresponding files.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **File Maintenance**.

3 Select a file type and highlight its corresponding file.

To ensure that you selected the right file, click **Details** to review information about the file.

4 Choose to download, upload, remove, or refresh the file.

5 Click **Apply** or **OK**.

Back up and restore in FIPS mode

Back up and restore communication information for McAfee ESM devices in FIPS mode.

Primarily, you can use it if a failure requiresMcAfee 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 McAfee ESM is used by the secondary McAfee ESM to establish communication with the device initially. Once communication is established, the secondary McAfee ESM copies its public key to the device's authorized keys table. The secondaryMcAfee ESM then erases the private key for the primary McAfee ESM, and initiates communication with its own public or private key pair.

Task

1

1 Export the .prk file from the primary McAfee ESM

a On the system navigation tree of the primary McAfee ESM, select the device with communication information you want to back up, then click the **Properties** icon.

b Select **Key Management**, then click **Export Key**.

c Select **Backup SSH Private key**, then click **Next**.

d Type and confirm a password, then set the expiration date.

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 McAfee ESM.

e Click **OK** and then select the location to save the .prk file created by the McAfee ESM.

f Log off from the primary McAfee ESM.

2 Add a device to the secondary McAfee ESM and import the .prk file.

a On the system navigation tree of the secondary device, select the system or group level node you want to add the device to.

b From the actions toolbar, click **Add Device**.

c Select the type of device that you want to add, then click **Next**.

d Enter a name for the device that is unique in this group, then click **Next**.

e Enter the target IP address of the device, enter the FIPS communication port, then click **Next**.

f Click **Import Key**, browse to the previously exported.prk file, then click **Upload**.

g Type the password specified when this key was initially exported.

h Log off from the secondary McAfee ESM.

Back up system settings

Specify when and how you want the system to back up your McAfee ESM settings. You can configure automatic backups by defining the frequency and timing of the backup, what to back up, and where to store the backup files. Or, you can back up settings manually.

Before you begin

Backups are only compatible with the current version of the device. You can't install a backup of a previous version on an updated McAfee ESM device.

By default, McAfee ESM automatically backs up your McAfee ESM settings every 7 days. The default backup location resides on the McAfee ESM device

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **ESM Management**, then click the **Maintenance** tab.

3 Click **Backup**.

4 Define the settings for the backup then click **OK**.

To conserve storage space and to ensure the ability to restore reliable settings and data, schedule data and log backups to a secondary host storage platform.

Option	Definition
Backup Frequency	When you add McAfee ESM devices, the system enables the **Backup and Restore** function to perform a backup every 7 days. You can change the frequency or disable the backup.
Back up Data For	Select what you want to include in the backup.
Backup Location	Select where you want the backup saved: • **ESM** — Saved on McAfee ESM. • **Remote Location** — Saved in the location you define in the fields that become active. If you save a copy of all McAfee ESM system data manually, you must select this option. When you back up to a Common Internet File System (CIFS) share, use a slash (/) in **Remote Path**.
Backup Now	Manually back up McAfee ESM settings and events, flows, and logs (if selected). Click **Close** when the system completes the backup successfully.

Back up ELM settings

Back up current Enterprise Log Manager (ELM) settings so that 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.

Before you begin

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

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select the ELM, then click the **Properties** icon ⚙.
3. Select **ELM Information**, then click **Backup & Restore**.
4. Indicate the backup frequency and location. Then, test the connection.

Restore settings

When McAfee ESM fails, restore settings to a previous state.

Before you begin

Back up McAfee ESM settings regularly.

Task

1. From the McAfee ESM dashboard, click ☰ and select **System Properties**.
2. Click **ESM Management** | **Maintenance** | **Restore Backup**.
3. Select the type of restore you need to perform.
4. 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. McAfee ESM is offline until the full restore is completed. During this time, McAfee ESM tries to reconnect every 5 minutes.

Restore device configuration files

Restore SSH, Network, SNMP, and other configuration files backed up on McAfee ESM for each device.

Before you begin

Back up device configuration files onMcAfee ESM.

Task

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**.

Retrieving ELM data

To retrieve data from the Enterprise Log Manager (ELM), you must create search and integrity-check jobs.

Run an integrity-check job to determine whether the defined files have changed since they were originally stored. This can alert you to unauthorized changes to critical system or content files. The results of this check show which files were changed. If no files were changed, the system notifies you that the check was successful.

You can complete up to 50 searches and integrity-check jobs at one time. If more than 50 jobs exist on the system, the system indicates that your search can't be performed. You can delete existing searches on the system so that the system can perform new searches. Work with your system administrator to delete existing searches or integrity-check jobs to perform your search.

Running complex searches over long time spans can cause the search process to stop working. Consider breaking these searches into smaller time spans.

Once you initiate a search, it continues to run until it finishes or reaches a set limit.

9 Tuning your configuration

Contents

How McAfee Application Data Monitor works

McAfee Application Data Monitor tracks use of sensitive data on the network, analyzing underlying protocols, session integrity, and application contents.

When McAfee Application Data Monitor 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, McAfee Application Data Monitor provides visibility into threats that masquerade as legitimate applications.

McAfee Application Data Monitor can detect when sensitive information is transmitted inside email attachments, instant messages, file transfers, HTTP posts, or other applications. Customize McAfee Application Data Monitor detection capabilities by defining your own dictionaries of sensitive and confidential information. McAfee Application Data Monitor can then detect these sensitive data types, alert appropriate personnel, and log the transgression to maintain an audit trail.

McAfee Application Data Monitor 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

McAfee Application Data Monitor accepts rule expressions and tests them against monitored traffic, inserting records into the database event table 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 the database query tables for every triggered rule. It stores a text representation of the protocol stack in the query table's packet field.

McAfee Application Data Monitor can generate the following types of event:

- **Metadata** - McAfee Application Data Monitor generates one metadata event for each network transaction, with details such as addresses, protocol, file type, file name. McAfee Application Data Monitor 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, McAfee Application Data Monitor 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; McAfee Application Data Monitor places them 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 are rare; McAfee Application Data Monitor places them 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 in 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 McAfee Application Data Monitor time zone

The system uses the time zone you set for McAfee Application Data Monitor to evaluate rules.

The default time zone is set to GMT but the McAfee Application Data Monitor code expects the device to be set to your time zone. Set the time zone to your time zone so that rules use your time trigger not the GMT time zone.

Task

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 McAfee Application Data Monitor queries in a session. Some event rules might be password-related. You can select whether you want the passwords to display on the Session Viewer.

Task

1 On the system navigation tree, select **ADM Properties**, then click **ADM Configuration**.

By default, passwords do not display.

2 Click **Passwords**, select **Enable password logging**, then click **OK**.

Manage McAfee Application Data Monitor selection rules

The system uses *selection rules* as filters to determine which packets a virtual device processes. You can add, edit, and delete selection rules.

Place rules that will match the most packets first in the order. This reduces the average number of times a packet is parsed and therefor reduces CPU usage.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the device, then click the **Properties** icon ⚙.

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

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

There can be up to 4 McAfee Application Data Monitor interface filters. Each filter can only be applied to one McAfee Application Data Monitor virtual device at a time.

McAfee® Application Data Monitor rules syntax

McAfee Application Data Monitor rules provide a set of literals (numbers, strings, regular expressions, IP addresses, MAC addresses, and Booleans), similar to C expressions.

You can compare string terms with string and Regex literals to test their content but they can also be compared with numbers to test their length. You can only compare numeric, IP address, and MAC address terms 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 9-1 Operators

Operator	Description	Example
&&	Logical AND	protocol = = http && type = = image/gif
||	Logical OR	time.hour < 8 || time.hour > 18
^ ^	Logical XOR	email.from = = "a@b.com" ^^email.to = = "a@b.com"
!	Unary NOT	! (protocol = = http | | protocol = = ftp)
= =	Equal	type = = application/pdf
! =	Not equal	srcip ! = 192.168.0.0/16

Table 9-1 Operators *(continued)*

Operator	Description	Example
>	Greater	objectsize > 100M
> =	Greater or equal	time.weekday > = 1
<	Less	objectsize < 10K
< =	Less or equal	time.hour < = 6

Table 9-2 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 9-3 Type operator compatibility

Type	Operators	Notes
Number	= =, ! =, >, > =, <, < =	
String	= =, ! =	Compare content of string with String/Regex
String	>, > =, <, <=	Compare length of string
IPv4	= =, ! =	
MAC	= =, ! =	
Bool	= =, ! =	Compare against true/false, also supports implied comparison with true, for example the following tests whether the email.bcc term occurs: email.bcc

Table 9-4 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
S	End of line
	The start of line and end of line anchors (^ and $) don't work for objcontent.

POSIX character classes	
[:alunum:]	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

POSIX character classes	
[:word:]	Word characters
[:xdigit:]	Hexadecimal Digit

McAfee® Application Data Monitor rule term types

McAfee Application Data Monitor rules contain terms that can be IP addresses, MAC addresses, numbers, strings, or a Boolean.

In addition, there are two extra literal types: regular expressions and lists. A term of a specific type can 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 ...).

Exceptions to this rule are:

- 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
- A string term can be compared against a regular expression. The following rule triggers if a password only contains lowercase letters: Password == /^[a-z]+$/
- 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	• 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	• MAC address literals are written using standard notation, as with IP addresses, they are not enclosed in quotes: aa:bb:cc:dd:ee:ff
Numbers	• All numbers in McAfee Application Data Monitor 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	• 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, the following rule does not trigger: email.from == “@somewhere.com” • To match only a part of a term, use a regular expression literal instead. String literals must be used when possible because they are more efficient. All email address and URL terms are normalized before matching so it is not needed to take account of things like comments in email addresses.
Booleans	• The Boolean literals are true and false.

Type	Format description
Regular expressions	• Regular expression literals use the same notation as languages like JavaScript and Perl, enclosing the regular expression in forward slashes: /[a-z]+/ • Follow regular expressions with standard modifier flags, though "i" is the only one currently recognized (case-insensitive): /[a-z]+/i • Use the POSIX Extended syntax for regular expression literals. 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 in the term unless anchor operators are applied in the regular expression. The following rule triggers if an email is seen with an address of “someone@somewhere.com”: email.from == /@somewhere.com/
Lists	• List literals consist of one or more literals enclosed in square brackets and separated by commas: [1, 2, 3, 4, 5] • Lists might contain any kind of literal, including other lists: [192.168.1.1, [10.0.0.0/8, 172.16.128.0/24]] • Lists must only contain one 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 (!=), 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: Srcip == [192.168.1.1, 192.168.1.2, 192.168.1.3] • It is equivalent to: Srcip == 192.168.1.1 || srcip == 192.168.1.2 || srcip == 192.168.1.3 • When used with the not-equal (!=) operator, the expression is true if the term doesn't match all literals in the list. The following rule triggers if the source IP address is not 192.168.1.1 or 192.168.1.2: Srcip != [192.168.1.1, 192.168.1.2] • It is equivalent to: Srcip != 192.168.1.1 && srcip != 192.168.1.2 • Lists might also be used with the other relational operators, though it doesn't make much sense. The following rule triggers if the object size is greater than 100 or if the object size is greater than 200: objectsize > [100, 200] • It is equivalent to: objectsize > 100 || objectsize > 200

McAfee® Application Data Monitor rule metric references

Use the following metric references when adding McAfee Application Data Monitor rules.

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, but, be detected using Object Type (objtype)
Object Type (Number)	Specifies the type of the content as determined by McAfee Application Data Monitor (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)

Property or term	Description
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 address 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)

Protocol-specific properties

In addition to providing properties that are common across most protocols, McAfee Application Data Monitor also provides protocol-specific properties that can be used with McAfee Application Data Monitor rules.

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 9-5 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	Referrer		
	URL		
	All HTTP headers		

Table 9-6 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 9-7 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***

Protocol anomalies

Beyond the common properties and protocol-specific properties, McAfee® Application Data Monitor 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 a McAfee® Application Data Monitor rule.

Table 9-8 IP address

Term	Description
ip.too-small	IP address packet is too small to contain a valid header.
ip.bad-offset	IP address data offset goes past end of packet.
ip.fragmented	IP address packet is fragmented.
ip.bad-checksum	IP address packet checksum doesn't match data.
ip.bad-length	IP address packet totlen field goes past end of packet.

Table 9-9 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 is already 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 9-10 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.

How McAfee Application Data Monitor dictionaries work

When writing McAfee Application Data Monitor 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.

McAfee Application Data Monitor 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 with 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 McAfee Application Data Monitor 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 McAfee ESM.

3 Assigning the dictionary to a rule.

Setting up McAfee Application Data Monitor dictionaries

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 defaults to Boolean true if not present.

Values in a single or double column dictionary must be one of the supported McAfee Application Data Monitor types: String, Regular Expression, Number, IPv4, IPv6, or MAC. McAfee Application Data Monitor dictionaries must follow these formatting guidelines:

Type	Syntax Rules	Examples	Content Matched
String	• Strings must be enclosed in double quotes • Double quotes found in a String must be escaped using the backslash character before each quotation mark	“Bad Content” “He said, \”Bad Content\””	Bad Content He said, “Bad Content”
Regular Expression	• Regular expressions are enclosed with single forward slashes • Forward slashes and reserved regular expression characters in the regular expression must be escaped with the backslash character	/[Aa]pple/ /apple/i / [0–9]{1,3}\.[0–9]{1,3}\.[0–9]\.[0–9]/ /1\/2 of all/	Apple or apple Apple or apple IP addresses: 1.1.1.1 127.0.0.1 1/2 of all
Numbers	• Decimal Values (0–9) • Hexadecimal Values (0x0-9a-f) • Octal Values (0–7)	Decimal Value Hexadecimal Value Octal Value	123 0x12ab 0127
Booleans	• Can be true or false • All lowercase	Boolean Literals	true false
IPv4	• 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 McAfee Application Data Monitor type. This means that different types (string, regex, IPv4) cannot be mixed and matched in a single McAfee Application Data Monitor dictionary file.
- They can contain comments. All lines starting with the pound character (#) are considered a comment in an McAfee Application Data Monitor 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 in them.
- They must be edited or created outside of McAfee ESM with a text editor of your choice. They can be imported or exported from McAfee ESM to facilitate changing or creating McAfee Application Data Monitor dictionaries.

Reference McAfee Application Data Monitor dictionaries

When importing McAfee Application Data Monitor dictionaries into McAfee ESM, see them when writing rules.

Before you begin

Import the McAfee Application Data Monitor dictionary to the McAfee ESM.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the ADM and then open the **Policy Editor**.

3 Under **Rule Types**, select **ADM** the of the **Policy Editor**, .

4 Click **New** | **ADM Rule**.

5 Add the requested information and drag and drop a logical element to the **Expression Logic** area.

6 Drag and drop the **Expression Component** icon onto the logical element.

7 Configure the expression component, selecting the ADM **Dictionary**.

McAfee Application Data Monitor dictionary examples

McAfee Application Data Monitor can match object content or other metrics or properties with a single column dictionary for true or false (exists in the dictionary or does not exist in the dictionary).

Table 9-11 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 with 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 9-12 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 with 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 and 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”

Manage McAfee Application Data Monitor dictionaries

Once you set up and save a McAfee Application Data Monitor dictionary, you must import it to McAfee ESM. You can also export, edit, and delete it.

Task

1 On the **Policy Editor**, click **Tools**, then select **ADM Dictionary Manager**.

Manage ADM Dictionaries lists 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**.

When you delete a dictionary, any attempt to roll out a rule set with rules that reference this dictionary fails to compile. If this dictionary is assigned to a rule, either rewrite the rule so it does not see the dictionary, or do not continue with the deletion. If there is a discrepancy between what you selected in the **Key Type** and **Value Type** fields and what the file contains, the system indicates invalid data.

How McAfee® Database Event Monitor works

McAfee Database Event Monitor 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, McAfee Database Event Monitor generates an alert. In addition, all transactions are logged for use in compliance.

McAfee Database Event Monitor 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.

McAfee Database Event Monitor 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 McAfee Database Event Monitor 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.

Operating system	Database	Device
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
Mainframe	DB2/zOS	All versions
AS400	DB2	All versions

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 McAfee Database Event Monitor license

The McAfee Database Event Monitor device comes with a default license. If you change the capabilities of the McAfee Database Event Monitor, McAfee sends you a new license in an email message and you must update it.

Task

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 McAfee Database Event Monitor.

Configure McAfee Database Event Monitor

Configure McAfee Database Event Monitor to reduce the load.

Task

1 On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.

2 When the McAfee Database Event Monitor device and its configuration files are out of sync, click **Sync Files** to write the configuration files to the device.

3 Click **Advanced**, then define the following settings:

Option	Definition
Log file detail level	Set the level of log detail sent from the agent to the manager: **Information**, **Warn**, and **Debug**.  If you select **Debug**, the information is detailed and can consume a great deal of disk space.
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 from the agent to the manager. 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.  Multiple IP addresses, Port, and VLAN settings can 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.
Shared memory	Choose the buffer size 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 device is read and those events are parsed. If you select **EDB**, events are collected from the database.

4 Deselect any of these options:

Option	Definition
McAfee Firewall packet capture	Provides a faster way to parse database data.
Transaction tracking	Tracks database transactions and auto reconcile changes. Deselect to increase 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 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 speed.
Local host auditing	Audits local hosts to track unknown access paths into the database and send events in real time. Deselect to increase speed.
Query parsing	Performs query inspections. Deselect to increase speed.
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 speed.
Bind variable support	Reuses the Oracle bind variable over and over without incurring the overhead of reparsing the command each time it's executed.

5 To apply the configuration settings to the McAfee Database Event Monitor device, click **Apply**.

Defining actions for McAfee Database Event Monitor events

Define McAfee® Database Event Monitor actions and operations for events, which the device uses to filter rules and data access policies. Set operations for default and custom actions.

McAfee Database Event Monitor comes with the following default actions and operations:

- **none**
- **ignore**
- **discard**
- **scripts**
- **reset**

If you select **Script** as the operation, an alias name (SCRIPT ALIAS) is required, selecting 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. McAfee Database Event Monitor provides a sample bash script /home/auditprobe/conf/sample/process_alerts.bash to show how the criticality action can be captured in a script.

When working with actions and operations, consider the following:

- Actions appear in order of priority.
- No event actions occur (such as sending an SNMP trap or page) unless you specify as alert actions.
- 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 DEM actions on page 158

Add DEM actions

Select Database Event Monitor (DEM) actions for rules in the **Policy Editor**.

Task

1 On the system navigation tree, click the **Policy Editor** icon , then click **Tools** | **DEM Action Manager**.

DEM existing actions appear in order of priority.

You can't change the priority order of default actions. The default operation for a custom action is **None**.

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**.

See also

Defining actions for McAfee Database Event Monitor events on page 157

Edit DEM custom actions

Once you add actions to the Database Event Monitor (DEM) action management list, can change its name or priority.

Task

1 On the system navigation tree, click the **Policy Editor** icon , then click **Tools** | **DEM Action Manager**.

2 Click the custom action 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.

Set operations for DEM actions

All rule actions have default operations. When you add a custom Database Event Monitor (DEM) action, the default operation is **None**. You can change the operation of any action to **Ignore**, **Discard**, **Script**, or **Reset**.

Task

1 On the system navigation tree, select **DEM Properties**, then click **Action Management**.

2 Highlight the action, then click **Edit**.

You can't delete a custom action or change the priority order of default actions.

3 Change the operation of the rule action as follows:

Option	Definition
Operation	Select what you want this action to do if the rule triggers an event. The options are: • **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.

4 Click **OK**.

DEM rule metric references

Here is a list of metric references for DEM rule expressions, which are available on the **Expression Component** page when you are adding a DEM rule.

Name	Definition	Database Types
Application Name	The name that identifies the database type to which the rule applies.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PIServer, InterSystems Cache
Begin Time	Start timestamp of the query.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Begin Time Skew	Captures the server clock time skews.	MSSQL, Oracle, DB2, Sybase, MySQL, PostgreSQL, Teradata, PIServer, InterSystems Cache
Client IP	Client's IP address.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Client Name	Name of the client machine.	MSSQL, Oracle, DB2, Sybase, Informix, PIServer, InterSystems Cache
Client PID	Process ID assigned by the operating system to the client process.	MSSQL, DB2, Sybase, MySQL
Client Port	Port number of the client socket connection.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Command Name	Name of the MySQL command.	MSSQL, Oracle, DB2, Sybase, Informix
Command Type	Type of MySQL command: DDL, DML, Show or Replication.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache

Name	Definition	Database Types
Data In	Total number of bytes in the inbound query packet.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Data Out	Total number of bytes in the outbound result packets.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Database Name	Name of the database being accessed.	MSSQL, DB2, Sybase, MySQL, Informix, PostgreSQL, PIServer, InterSystems Cache
End Time	End of the completion timestamp query.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Error Message	Contains the message text associated with the SQLCODE and SQLSTATE variables in the SQL Communication Area (SQLCA) data structure which provides information about the success or failure of requested SQL statements.	DB2, Informix
Message Number	A unique message number assigned by the database server to each error.	MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache
Message Severity	Severity level number between 10 and 24, which indicates the type and severity of the problem.	MSSQL, Sybase, Informix
Message Text	Full text of the message.	MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache
Network Time	Time taken to send the result set back to the client (response_time - server_response_time).	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
NT Client Name	Windows machine name from which the user logged in.	MSSQL
NT Domain Name	Windows domain name from which user logged in.	MSSQL
NT User Name	Windows user login name.	MSSQL
Object Name		MSSQL, Oracle, DB2, Sybase, MySQL, Informix
OSS User Name		Oracle
Package Name	A package contains control structures used to execute SQL statements. Packages are produced during program preparation and created using the DB2 subcommand BIND PACKAGE.	DB2
Packets In	Number of packets comprising the query.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache

Name	Definition	Database Types
Packets Out	Number of packets comprising the return result set.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Password		MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, InterSystems Cache
Password Length		MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, InterSystems Cache
Query Block Size	Query block is the basic unit of transmission for query and result set data. Specifying the query block size enables the requester, which may have resource constraints, to control the amount of data that is returned at any one time.	DB2, Informix
Query Exit Status	Exit status of a query.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache
Query Number	A unique number assigned to each query by the AuditProbe monitoring agent starting with zero for the first query and incrementing by one.	MSSQL, Oracle, DB2, Sybase, MySQL, PostgreSQL, Teradata, PIServer, InterSystems Cache
Query Text	The actual SQL query sent by the client.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Query Type	An integer number assigned to different type of queries.	MSSQL, Oracle, Sybase
Real User Name	Client user login name.	
Response Content		MSSQL, Oracle, DB2, Sybase, MySQL, Informix
Response Time	End-to-end response time of the query (server_response_time + network_time).	MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache
Return Rows	Number of rows in the return result set.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache.
Security Flag	Security flag metric whose value is set to 1 (TRUSTED) or 2 (UNTRUSTED) when access policy file criteria specified by the administrator is met. Value of 3 indicates that policy file criteria were not met. Value of 0 indicates that security monitoring has not been turned on.	MSSQL, Oracle, DB2, Sybase, MYSQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems
Security Mechanism	The security mechanism that is used to validate the user's identity (for example, User ID and password).	DB2
Server IP	IP address of the database server host.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache

Name	Definition	Database Types
Server Name	This is the name of the server. The host name is assigned as the server name by default.	MSSQL, Oracle, DB2, Sybase, Informix, PIServer, InterSystems Cache
Server Port	Port number of the server.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache
Server Response Time	Initial response from the database server to the client query.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
Severity Code		DB2
SID	Oracle system identifier.	Oracle, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache
SPID	Database system process ID assigned to each unique connection/session.	MSSQL, Sybase
SQL Code	Whenever an SQL statement executes, the client receives a SQLCODE which is a return code that provides additional DB2-specific information about an SQL error or warning: • SQLCODE EQ 0, indicates execution was successful. • SQLCODE GT 0, indicates execution was successful with a warning. • SQLCODE LT 0, indicates execution was not successful. • SQLCODE EQ 100, indicates that no data was found. The meaning of SQLCODEs other than 0 and 100 varies with the particular product implementing SQL.	
SQL Command	Type of SQL command.	
SQL State	DB2 SQLSTATE is an additional return code that provides application programs with common return codes for common error conditions found among the IBM relational database systems.	DB2
User Name	Database user login name.	MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache

How McAfee Database Event Monitor rules work

McAfee® Database Event Monitor captures and normalizes network packet information.

Create McAfee® Database Event Monitor rules using logical and regular expressions for pattern matching 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. Craft filter expressions carefully, not only the syntax but also by making sure that the system supports the metric.

McAfee® Database Event Monitor contains the default rules (listed below).

Default compliance rules monitor significant database events such as logon/logoff, DBA-type activity such as DDL changes, suspicious activity, and database attacks typically required to achieve compliance requirements. Enable or disable each default rule and set the value of each rule's user-definable parameters.

Rule types	Description
Database	Default rules for each supported database type and common regulations, such as SOX, PCI, HIPAA, and FISMA. Enable or disable the default rules and set user-definable parameters for each rule. Application protocols and messages vary, which means normalized data (metrics) can vary for each application. Rules can include both Logical and Regular Expression operators. A Rule Expression can be applied against one or more metrics available for the application.
Data access	Rules that rack unknown access paths into the database and send alerts in real time. Create data access rules to track common violations in database environments, such as application developers accessing production systems using application logon IDs.
Discovery	Rules that identify an exception list of database servers, of the types supported by McAfee ESM, that are on the network but are not being monitored. Discovery rules allow security administrators to discover new database servers added to the environment and illegal listener ports opened to access data from databases. Discovery rules are out-of-box rules, which you cannot add or edit. When you enable the discovery option on database servers, the system uses these rules to search for database servers that are on the network, but are not listed under the McAfee® Database Event Monitor device.
Transaction tracking	Rules that track database transactions and auto-reconcile changes. For example, use these rules to automate tracking and reconciling database changes with authorized work orders in your change ticketing system. For example: The DBA executes the start tag stored procedure (spChangeControlStart in this example) in the database performing the work before actually beginning the authorized work. Transaction tracking allows the DBA to include up to 3 optional string parameters as arguments to the tag in the correct sequence: **1** ID **2** Name or DBA Initials **3** Comment For example, `spChangeControlStart '12345', 'mshakir', 'reindexing app'` When the system observes the execution of the spChangeControlStart procedure, it logs both the transaction and parameters (ID, Name, Comment) as special information. Once the work completes, 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 system 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 report by transactions and search by ID, which could be the change control number. Use transaction tracking to log start and end of a trade execution or begin and commit statements to report by transactions instead of queries.

Set up data access rules

Set up access rules to track unknown access paths into the database and send events in real time. For example, track common violations in database environments, such as application developers accessing production systems using application logon IDs.

Task

1 In the **Rule Types** pane on the **Policy Editor**, select **DEM** | **Data Access**.

2 Do one of the following:

- Select **New**, then click **Data Access Rule**
- Select the rule in the rules display pane, then click **Edit** | **Modify**.

3 Fill in the information, then click **OK**.

Working with sensitive data masks

Sensitive data masks prevent unauthorized viewing of data by replacing the sensitive information with generic strings, called the *mask*. When you add a McAfee Database Event Monitor device, the system adds standard sensitive data masks to the McAfee ESM database. You can also add or change masks.

Standard masks include:

- Sensitive mask name: Credit Card Number Mask

  Expression: ((4\d{3})|(5[1–5]\d{2})|(6011))-?\d{4}-?\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

  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: ********

Manage sensitive data masks

To protect sensitive McAfee ESM information, add, change, or remove sensitive data masks.

Task

1 On the system navigation tree, select **DEM Properties**, then click **Sensitive Data Masks**.

2 Select an option, then enter the requested information.

- Name the sensitive data mask.
- Type a REGEX expression that conforms to Perl-Compatible Regular Expression (PCRE) syntax.

- Select an option.

  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.

- Type the masking pattern that must appear in place of the original value.

3 Click **OK**, then click **Write** to add the settings to the DEM.

Managing user identification

Capture the real user name, if it exists anywhere in the query, using REGEX patterns.

When you add a DEM device, the system adds defined identifier rules to the McAfee ESM database.

- 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 logons to McAfee ESM.

Add user identifier rules

To associate database queries with individuals, use existing user identifier rules or add rules.

Task

1 On the system navigation tree, select **DEM Properties**, then click **Identifier Management**.

2 Click **Add**, then enter the information requested:

- Type a name for the identifier rule.
- Type a REGEX expression that conforms to PCRE syntax.

  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">`.

- Select the application (database type) where the information is observed.
- 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.

3 Click **OK**, then click **Write** to write the settings to the DEM.

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
UNIX/Linux (all version)	Greenplum	8.2.15
	Vertica	5.1.1-0
Mainframe	DB2/zOS	All versions
AS 400	DB2	All versions

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.

Manage database servers

Manage settings for all database servers for your Database Event Monitor (DEM) device. You can associate a maximum of 255 database servers with each DEM device.

Task

1 On the system navigation tree, select **DEM Properties**, then click **Database Servers**.

2 Select any of the available options.

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 McAfee ESM for later use.
Storage Pool	Click and select a storage pool if you want the data received sent to the ELM device.

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	Select the type of database. The remaining fields vary, based on what you select in this field. 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).
Database Server Name	Type a name for this database server. 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.
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 necessary. 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	Select one of the following (options available depend on database type selected): • **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	Click **Browse** and select the **RSA Key** file, or copy the key from the file and paste it in the **RSA Key** field. The McAfee ESM console accepts only RSA certificates of .pem file format with no password.

Option	Definition
Username	Type the user name for PI DAS logon. 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.

3 Click **OK**.

Manage database discovery notifications

The Database Event Monitor (DEM) can discover an exception list of unmonitored database servers, allowing you to discover database servers in the environment and illegal listener ports opened to access data from databases. When enabled, you receive notifications and choose whether to add the server to those monitored on your system.

Task

1 On the system navigation tree, select **DEM Properties**, then click **Database Servers** | **Enable**.

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**.

How McAfee ePolicy Orchestrator works as a device

You can add a McAfee ePO device to McAfee ESM, with its applications listed as secondary devices on the system navigation tree. Once authenticated, you can access functions from McAfee ESM, and assign McAfee ePO tags to source or destination IP addresses directly and to events generated by alarms.

You must associate McAfee ePO with the McAfee Event Receiver because the events are pulled from the receiver, not McAfee ePO.

You must have read permissions on the master database and McAfee ePO database to use McAfee ePO.

If the McAfee ePO device has a McAfee® Threat Intelligence Exchange (TIE) server, the system adds it automatically when you add the McAfee ePO device to McAfee ESM.

Start McAfee ePO from McAfee ESM

If you have an McAfee ePolicy Orchestrator McAfee ePO device or data source on McAfee ESM, and the McAfee ePO IP address is on your Local Network, you can start McAfee ePO from McAfee ESM.

Before you begin
Add a McAfee ePO device or data source to McAfee ESM.

Task

1 From the dashboard, open a view.

2 Select a result that returns source IP or destination IP data.

3 From the component menu ⋮, click **Actions** | **Launch ePO**.

- If you only have one McAfee ePO device or data source on the system and selected a source IP or destination IP, McAfee ePO starts.
- If you have multiple McAfee ePO devices or data sources on the system, select the one you want to access and McAfee ePO starts.

Assign McAfee ePolicy Orchestrator (McAfee ePO) tags to IP addresses

Assign McAfee ePO tags to events generated by alarms and views if alarms have McAfee ePO tags. You can also select one or more tags and apply them to IP addresses.

Before you begin

Verify that you have the following McAfee ePO privileges: **Apply, exclude, and clear tags** and **Wake up agents; view Agent Activity Log**:

Task

1 On the system navigation tree, select **ePO Properties**, then click **Tagging**.

2 Complete the requested information, then click **Assign**.

- Type a host name or IP address (supports comma-delimited list), then select one or more tags on the **Tags** list.
- Select to wake up the application to apply the tags immediately.
- Click **Assign** to apply the selected tags to the IP address.

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. The system prompts you for 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 McAfee ESM or when you set up its connection settings.

2 Enter your credentials.

McAfee Risk Advisor data acquisition

You can specify multiple McAfee ePO servers from which to acquire McAfee Risk Advisor data. The data is acquired through a database query from the McAfee ePO 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. The system merges all McAfee ePO and McAfee Risk Advisor; duplicate IPs receive the highest score. The system sends the merged list, with low and high values, to any McAfee Advanced Correlation Engine (ACE) devices used for scoring SrcIP and DstIP fields.

When you add McAfee ePO, the system prompts whether you want to configure McAfee Risk Advisor data. If you click **Yes**, the system creates and rolls out a data enrichment source and two ACE scoring rules (if applicable). If you want to use the scoring rules, you must create a risk correlation manager.

McAfee® Threat Intelligence Exchange (TIE) integration

McAfee® Threat Intelligence Exchange (TIE) verifies the reputation of executable programs on the endpoints connected to these files.

When you add a McAfee ePO device to McAfee ESM, the system automatically detects if a Threat Intelligence Exchange server is connected to the device. If it is, McAfee ESM starts listening in on the DXL and logging events.

A delay might occur when McAfee ESM connects to the DXL.

When the system detects aThreat Intelligence Exchange server, they system adds Threat Intelligence Exchange watchlists, data enrichment, and correlation rules automatically and enables Threat Intelligence Exchange alarms. You receive a visual notification, which includes a link to a summary of changes. The system also notifies you if the Threat Intelligence Exchange server is added to the McAfee ePO server after the device is added to McAfee ESM.

Once Threat Intelligence Exchange generates events, you can view their execution history and select the actions to take on the malicious data.

Correlation rules

The system optimizes correlation rules for Threat Intelligence Exchange data. They generate events that you can search and sort through.

- Threat Intelligence Exchange — McAfee GTI reputation changed from clean to dirty
- Threat Intelligence Exchange — Malicious file (SHA-1) found on increasing number of hosts
- Threat Intelligence Exchange — Malicious file name found on increasing number of hosts
- Threat Intelligence Exchange — Multiple malicious files found on single host
- Threat Intelligence Exchange — Threat Intelligence Exchange reputation changed from clean to dirty
- Threat Intelligence Exchange — Increase in malicious files found across all hosts

Alarms

McAfee ESM has two alarms that might trigger when the system detects important Threat Intelligence Exchange events.

- **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 Threat Intelligence Exchange 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 without expiration.

Threat Intelligence Exchange execution history

You can view the execution history for any Threat Intelligence Exchange event, which includes a list of the IP addresses that have tried to execute the file. 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.

View Threat Intelligence Exchange execution history and set up actions

McAfee® Threat Intelligence Exchange (TIE) execution history displays systems that have executed the file associated with selected events.

Before you begin

A McAfee ePolicy Orchestrator device with an attached Threat Intelligence Exchange server on McAfee ESM must exist.

Task

1. On the system navigation tree, click the McAfee ePolicy Orchestrator device.
2. On the views drop-down list, select **Event Views** | **Event Analysis**, then click the event.
3. Click ⋮, then select **Actions** | **TIE Execution History**.
4. 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 list, then select an option to open the McAfee ESM device.
6. Set up the action you selected.

Event Receivers

Contents

Security Device Event Exchange (SDEE)

The Security Device Event Exchange (SDEE) format describes how to represent 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*; 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.

SDEE uses the *pull* model, which means the Receiver periodically contacts the SDEE provider and requests events generated since the time of the last event was requested. Each time the Receiver requests events from the SDEE provider, the system processes and stores those events into the Receiver's event database, ready McAfee ESM retrieval.

Add SDEE providers to Receivers as data sources by selecting Cisco as the vendor and IOS IPS (SDEE) as the data source model.

The Receiver extracts the following from SDEE/CIDEE events:

- 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
- McAfee ESM event ID is calculated from the SDEE signature ID and the CIDEE subsignature ID using the following formula: `ESMI ID = (SDEE ID * 1000) + CIDEE sub-ID`

  If the SDEE signature ID is 2000 and the CIDEE subsignature ID is 123, the McAfee ESM 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 system uses the current date and time as a starting point for requesting events. Future connections request all events since the last successful pull.

Reinitialize secondary high availability Receivers

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

Task

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**.

Reset high availability devices

To reset high availability Receivers to the state before being set up as high availability devices, you can do so on the McAfee ESM console or, if communication with the Receivers fails, on the LCD menu.

- Do one of the following:
  - Reset a Receiver on McAfee ESM

    Both Receivers restart after a timeout of 5 minutes, returning the MAC addresses to their original values.

    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**.
  - Reset the primary or secondary Receiver on the LCD menu
    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.

Switch high availability Receiver 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 associates 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

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:
   - McAfee ESM instructs the secondary Receiver to start using the shared data source IP address and collecting data.
   - The secondary Receiver issues a Cluster Resource Manager (CRM) command to switch the shared IP address and MAC, and starts the collectors.
   - McAfee ESM pulls all alert and flow data from the primary Receiver.
   - McAfee ESM selects the secondary Receiver as the primary and selects the primary Receiver as the secondary.

Replace failed Receivers

If a secondary Receiver has a health problem that can't be resolved, you might need to replace it. When you receive the new Receiver, install it. When the IP addresses are set and the cables are plugged in, you can continue to bring the Receiver back into the high availability cluster.

Task

1. On the system navigation tree, select **Receiver Properties** for the high availability 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**.
4. If a high availability Receiver goes down for any reason, the writing of data sources, global settings, aggregation settings, and others appears to fail and an SSH error appears. 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, but, does not roll out. Do one of the following:
   - 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.

View Receiver throughput statistics

View Receiver usage statistics, which includes the incoming (Collector) and outgoing (parsed) 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

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.

Log devices

Contents

- *View message logs and device statistics*
- *View system or device logs*

Set up communication with ELM

If you intent to send data from this device to the ELM, you must identify the ELM IP address and sync the device with the ELM.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the device, then click the **Properties** icon ⚙.

3 Assign an IP or sync devices.

- Click **<device> Configuration**, click **ELM IP**, and enter a new IP.
- If the device or the ELM has been replaced, click **Sync Device**. Syncing the ELM re-establishes the SSH communication between the two devices, using the key for the new device with the previous settings.

Set up default logging pool

Set up devices to send their event data to the ELM by configuring default logging pools.

Devices do not send events to the ELM until after their aggregation time periods have expired.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Configuration** | **Logging**.

Option	Definition
Log Configuration	Select **Logging** to enable it.
Logging	Click to access **ELM Logging Options**.
ELM Logging Options page	Select the storage pool on the ELM that you want the data logged on.
Device - ELM Association	If you haven't selected the ELM you want to log the data on, confirm that you want to do this. Once you make this association, you cannot change it.
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	If you don't have any ELM storage pools, go to**ELM Properties** | **Storage Pools** to add them.

Manage logs

Select the events you want saved in the event log.

Task

1 On the system navigation tree, select **System Properties**, then click **ESM Management**.

2 Click **Manage logs** and then select the event types you want to log.

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 with device status information.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the device, then click the **Properties** icon ⚙.

3 Click **<device> Management**.

4 Select an option.

- Click **View Log** to see system messages, then click **Download Entire File** to download the data.
- Click **View Statistics** to see device performance statistics such as Ethernet interface, ifconfig, and iptables filter.
- Click **Device Data** to download a .tgz file that contains device status data.

View system or device logs

System and device logs track events on the devices. View the logs to see a detailed list of events by device or for McAfee ESM.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 View system logs.

a On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

b On **System Properties**, click **System Log**.

c Set a time range and select whether to include archived partitions, then click **View**.

On the System Log page, you can refine your data selections or export the data to a plain text file.

3 View device logs.

a On the system navigation tree, select the device, then click the **Properties** icon ⚙.

b Click **Device Log**.

c Set a time range and select whether to include archived partitions, then click **View**.

On the Device Log page, you can refine your data selections or export the data to a plain text file.

How virtual devices work

Use virtual devices to monitor traffic, compare traffic patterns, and for reporting.

Purpose and benefits

Use virtual devices to:

- Compare traffic patterns against rule sets. For example, set up virtual devices to look at web traffic ports and set up policoes 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.

The number of virtual devices that you can add to an McAfee Application Data Monitor varies by the model.

How McAfee ESM uses selection rules

McAfee ESM uses selection rules 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 McAfee Application Data Monitor itself then processes it, as a default, if no selection rules are matched on any virtual devices.

Things to note for IPv4 virtual devices:

- The system sorts all packets for a single connection 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.
- The system sorts invalid packets (a packet that is not setting up a connection or part of an established connection) to the base device. For example, you have a virtual device that looks for packets with a source or destination port of 80. When an invalid packet comes through with a port of 80, the system sorts it 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 the system lists selection rules matters, because the first time a packet matches a rule, the system automatically routes that packet to that virtual device for processing. For example, you add 4 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 system compares packets coming into the McAfee Application Data Monitor to the selection rules for each virtual device in the order that the virtual devices are set up. So, the order in which the system checks virtual devices matters. 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.

McAfee Application Data Monitor virtual devices

McAfee Application Data Monitor virtual devices monitor traffic on an interface. There can be up to 4 McAfee Application Data Monitor interface filters on your system. Each filter can be applied to only 1 virtual device at a time. If a filter is assigned to a McAfee Application Data Monitor virtual device, it does not appear on the list of available filters until it is removed from that device.

Add virtual devices

You can add virtual devices to your McAfee Application Data Monitor devices, and set rules that determine the packets that each virtual device processes.

Before you begin

Verify that your McAfee Application Data Monitor devices support virtual devices.

Task

1 On the system navigation tree, select a McAfee Application Data Monitor device, then click the **Properties** icon .

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

3 Enter the information requested, then click **OK**:

- Name the virtual device and 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.
- Enable the device.
- If an ELM exists on your system and you want log data received by this virtual device on the ELM, select the storage pool.
- If zones exist, select the zone for this device.
- Define and determine the order of selection rules for the device.

4 Click **Write** to add the settings to the device.

How message settings work

Before you can send messages via email, text message (SNS), SNMP, or syslog, you must first connect McAfee ESM to your mail server. Then you can identify message recipients.

McAfee 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 McAfee 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, McAfee ESM sends each report line in a separate trap.

Syslog can also send CSV reports generated by McAfee ESM. Syslog sends query CSV reports one line per syslog message, with the data of each line of the query results arranged in comma-separated fields.

Connect email server

Configure the settings to connect McAfee ESM to the email server to deliver alarm and report messages.

Before you begin

Verify that you have administrator privileges or belong to an access group with user management privileges.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 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 McAfee ESM IP address to identify which McAfee ESM device generated the message.
From	Type your name.
Configure Recipients	Add, edit, or remove message recipients

4 Send a test email to verify the settings.

5 Click **Apply** or **OK** to save the settings.

Manage message recipients

You can define recipients for alarm or report messages and group email addresses to send messages to several recipients at once.

Task

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**.

Manage email groups

Group email recipients so that you can send one message to several recipients at one time.

Before you begin

Verify that recipients and their email addresses exist.

Task

1 On the system navigation tree, click the system, then click the **Properties** icon ⚙.

2 Click **Email Settings**, then click **Configure Recipients** | **Email Groups**.

3 Click **Add**, **Edit**, or **Remove** to manage the list of recipients groups.

4 Provide the information requested, then click **OK**.

Configure Remedy server settings

If you have a Remedy system set up, you must configure the Remedy settings so McAfee ESM can communicate with it.

Before you begin
Set up your Remedy system.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Custom Settings** | **Remedy**.

4 On the **Remedy Configuration** page, enter the information for your Remedy system, then click **OK**.

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.
User Name and Password	Type the credentials for the Remedy system if one is required.
To Address and From Address	Type the email addresses of the Remedy senders and recipients.

Managing network interfaces

Communicating with devices uses 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 interfaces with IP addresses for communication between McAfee ESM and the device. These device features require the use of a management interface:

- Full control of bypass network cards
- Use of NTP time synchronization
- Device-generated syslog
- SNMP notifications

Devices equipped with at least one management interface gives the device an IP address. With an IP address, McAfee ESM can access devices 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.

McAfee ESM interface bonding

McAfee ESM tries to auto-enable bonded NIC mode when it detects two management interfaces that both use 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.

Set up network interfaces

Define interface settings to determine how McAfee ESM connects to each device.

Task

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

2 Click the device's **Configuration** option, then click **Interface**.

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.

Option	Definition
Bypass NIC Configuration	Set bypass NIC so that the device passes all traffic, even if it is malicious. 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	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. use this setting with one of the following FTP clients: WinSCP 5.11, Filezilla, CoreFTP LE, or FireFTP.
HOME_NET	Type IP addresses, owned by your organization, that determine the direction of the flow traffic that the device collects.
Interfaces	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. 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. 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).
IPv6 Mode	Select whether to enable IPv6 mode. • **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 part 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 the system allows access between McAfee ESM and the devices.

4 Define the advanced network settings for the selected device (fields vary based on the selected device).

Option	Definition
ICMP Messages	Select either of the following options for ICMP. **Redirect** — If selected, McAfee ESM ignores redirect messages. **Dest Unreachable** — If selected, McAfee ESM generates a message when a packet can't be delivered to its destination for reasons other than congestion. **Enable Ping** — If selected, McAfee ESM sends an *Echo Reply* message in response to an *Echo Request* message sent to an IPv6 multicast/anycast address.
IPMI Settings	To manage McAfee ESM devices remotely through an IPMI card when an IPMI NIC is plugged into a switch, add the IPMI settings. • **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.

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

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**.

Option	Definition
VLAN	The number that identifies the VLAN in the system.
DHCP	Enables DHCP services for non-cloud environments. DHCP is useful if you need to reset the IP addresses for your network. If you are using a redundant ELM, redundancy stops working if the IP address of the redundant device is changed.
IPv4 or **IPv6**	IPv4 is selected by default. If you have IPv6 set to **Manual** or **Auto** on the **Network Settings** page, the **IPv6** option is enabled.
IP Address	The IP address for the VLAN.
Netmask	The **IPv4** netmask (disabled if the IP address is in IPv6 format).

4 Select the VLAN where you want to add the alias, then click **Add Alias**.

Option	Definition
VLAN	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	Shows whether the IP address is in IPv4 or IPv6 format.
IP Address	The IP address of the alias.
Netmask	The netmask (if the address is in IPv4 format).

5 Enter the requested information, then click **OK**.

Add static routes

A static route is a set of instructions about how to reach a host or network that is unavailable through the default gateway.

Task

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**.

Configure network settings

Configure McAfee ESM connects to your network by adding server gateway and DNS server IP addresses, defining proxy server settings, setting up SSH, and adding static routes.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the device, then click the **Properties** icon.

3 Click **Network Settings**.

4 Configure the settings on the **Main** tab.

Option	Definition
Interface 1, **Interface 2**	Defines available interfaces. At least one interface must be enabled.
Local Network	Defines the local network, including IP addresses or subnets. Values are separated by commas.
Enable SSH (not available in FIPS mode)	Enables secure communication over SSH. McAfee 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.
SSH Port	The port used for SSH connections.
Manage SSH keys	If you have enabled SSH connections, the systems listed can communicate through the SSH port. Deleting a system ID from the list disables communication.
IPv6 Settings	• **Off** — IPv6 mode is disabled. • **Auto** — the **Primary** and **Secondary IPv6** fields are disabled. Each host determines its address from the contents of received user advertisements. It uses the IEEE EUI-64 standard to define the network ID part of the address. • **Manual** — the **Primary** and **Secondary IPv6** fields are enabled.

5 Select the **Advanced** tab and then set up Internet Control Message Protocol (ICMP) messages and the Intelligent Platform Management Interface (IPMI).

Option	Definition
ICMP Messages	• **Redirect** — McAfee ESM ignores redirect messages. • **Dest Unreachable** — McAfee ESM generates a message when a packet can't be delivered to its destination for reasons other than congestion. • **Enable PING** — McAfee ESM sends an *Echo Reply* message in response to an *Echo Request* message sent to an IPv6 multicast/*anycast* address.
IPMI Settings	Sets the IPMI card to manage McAfee ESM devices if you have an IPMI NIC plugged into a switch. • **Enable IPMI Settings** — Enables access to IPMI commands. • **VLAN**, **IP Address**, **Netmask**, **Gateway** — Configures the network for the IPMI port.

6 If your network uses a proxy server, select the **Proxy** tab and then set up the connection to your McAfee ESM.

Option	Definition
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**	Information required to connect to the proxy server.
Basic Authentication	Implements basic authentication checking.

7 Select the **Traffic** tab and then click **Add** to define a maximum data output value for a network and mask to control the rate at which outbound traffic is sent.

Option	Definition
Network column	Shows the addresses of the networks on which the system controls outbound traffic.
Mask column	(Optional) Shows the masks for the network addresses.
Maximum Throughput column	Shows the maximum throughput you defined for each network.

8 To add or edit static routes, select the **Static Routes** tab and then click **Add** or **Edit**.

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 McAfee ESM and immediately takes effect when you click **Apply**. Upon applying changes, McAfee ESM reinitializes itself, causing all current sessions to be lost.

Option	Definition
IPv4 or **IPv6**	Determines whether this static route looks at IPv4 or IPv6 traffic.
Network	The network IP address for this route.
Mask	The network mask.
Gateway	The gateway IP address for this route.

Set up network traffic control

Define a maximum data output value for a network and mask to control the rate for sending outbound traffic for each device.

Limiting traffic can cause data loss.

Task

1. On the system navigation tree, select the system, then click the **Properties** icon .
2. Click **Network Settings**, then click the **Traffic** tab.
3. To add controls for a device, click **Add**, enter the network address and mask, set the rate in kilobits (KB), megabits (megabyte), or gigabits (GB), then select the rate per second for sending traffic, then click **OK.**

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

Network settings for IPMI ports

Set up IPMI ports on McAfee ESM or its devices to perform the following 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.
- Access IPMI commands like turn on and power status.
- Reset the IPMI card.
- Perform a warm and cold reset.

Set up IPMI port on McAfee ESM or devices

Configure the network for the IPMI port to set up IPMI on McAfee ESM or its devices.

Before you begin

The system must include an IPMI NIC.

Task

1. On the system navigation tree, select the system or any of the devices, then click the **System Properties** icon .
2. Access the **Network Settings Advanced** tab.
   - On McAfee 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 must 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**.

   When upgrading your device, a message might recommend that you change the password or rekey the device to configure the IPMI.

Set up network traffic control

Define a maximum data output value for a network and mask to control the rate for sending outbound traffic. Options include kilobits (KB), megabits (MB), and gigabits (GB) per second.

Limiting traffic can result in data loss.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.

3 Click **Network Settings**, then select the **Traffic** tab.

The table lists the existing controls.

4 Add controls for a device.

a Click **Add**.

b Set the network address, mask, and throughput rate.

If you set the mask to zero (0), all data sent is controlled.

Working with host names

Associate device host names with their corresponding IP addresses. Add, edit, remove, look up, update, and import host names, and 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 👤 at the bottom of view components.

If existing events are not tagged with a host name, the system searches the host table on McAfee ESM and tags the IP addresses with their host names. If the IP addresses don't appear 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 selected as **Auto Learned** and expires after the time designated in the **Entries expire after** field located below the host table on **System Properties** | **Hosts**. 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. 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.

Manage host names

Perform actions needed to manage host names, such as adding, editing, importing, removing, or looking them up. You can also set the expiration time for auto-learned hosts.

Task

1 On the system navigation tree, select **System Properties**, then click **Hosts**.

2 Select an option and enter the information requested.

- When adding a host, you can enter a host name up to 100 characters long and IP addresses in valid IPv4 or IPv6 notation including a mask.
- Change or delete existing host names.
- When setting up information for an internal network, you can look up the host name for an IP address.
- Import a tab-delimited list of IP addresses and host names.
- 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.

3 Click **Apply** or **OK**.

Import a list of host names

Import a text file that contains IP addresses and the corresponding host names.

Before you begin

Create a tab-delimited file with 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

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**.

Data that is entered manually does not expire. The system adds the new host data to the host table. The **Auto Learned** column for this data says **No**.

Set up Dynamic Host Configuration Protocol (DHCP)

Use Dynamic Host Configuration Protocol (DHCP) on IP networks to distribute network configuration parameters (such as IP addresses for interfaces and services) dynamically.

When you set up McAfee ESM to deploy in the cloud, the system enables DHCP enabled automatically and assigns an IP address.

When not in the cloud, you can enable and disable DHCP services on McAfee ESM, non-HA Receiver, ACE, and ELM if you have Device Management privileges. This helps if you need to reset the IP addresses for your network.

The system disables aliases when DHCP is enabled.

Task

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

2 Do one of the following:

- For McAfee 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 must restart the McAfee ESM server.

4 Click **Add VLAN**, type the **VLAN** number, then select **DHCP**.

5 Click **OK** then click **Apply**.

For devices other than Receivers, you must restart the McAfee ESM server.

Level 7 collection on McAfee Network Security Manager

Layer 7 data populates the McAfee Network Security Manager 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 Network Security Manager device

When adding the McAfee Network Security Manager device to McAfee ESM, select **Enable Layer 7 Collection** and set the delay on the **Add Device Wizard**.

Configuring a McAfee Network Security Manager device

After adding a McAfee Network Security Manager device to McAfee ESM, configure the connection settings for the device. You can select **Enable Layer 7 Collection** and set the delay.

Adding a McAfee Network Security Manager data source

To add a McAfee Network Security Manager data source to a Receiver, select McAfee in **Data Source Vendor** and **Network Security Manager - SQL Pull (ASP)** in **Data Source Model**. You can select **Enable Layer 7 Collection** and set the delay.

Data sources

Contents

Locate data source clients

You can have more than 65,000 clients. Use search to locate a specific data source client.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the Receiver, then click the **Properties** icon ⚙.

3 Click **Data Sources** | **Clients**.

4 In the **Search** field, enter the information you want to search for, then click **Search.**

Move data sources to another system

Move data sources from secured Receivers to Receivers on unsecured locations on different systems. Select data sources to be moved, save them and their raw data to a remote location, then you can import the data sources to another Receiver.

Before you begin

Verify that you have device management rights on both Receivers.

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 change correlation rules on the second Receiver, the correlation engine doesn't process those rules. When you transport correlation data, they system inserts those events from the file.

Task

1 On the system navigation tree, select **Receiver Properties**.

2 To select the data sources and remote location, do the following:

a Select the data source, then click **Edit.**

b Click **Advanced**, then select **Export in NitroFile.**

The data is exported to a remote location and is configured using profile. The system now copies raw data generated by this data source to the remote share location.

3 To create raw data file, do the following:

a Access the remote share location where the raw data is saved.

b 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).

4 To create a file that describes data sources, do the following:

a Select the data source, then click **Import**.

b Locate the file of data sources you moved and click **Upload**.

c 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.

The data sources are added to the second Receiver and accesses the raw data through the remote share profile.

5 To import raw data and data source files, do the following:

a On the second Receiver system navigation tree, access **Data Sources**, then click **Import**.

b Locate the file of data sources you moved and click **Upload**.

c 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.

6 Click **OK**.

Migrate data sources to Receivers

Reallocate or redistribute data sources between Receivers on the same system.

Migrate data sources to new Receivers and balance data sources between Receivers. Or, if you replace your Receiver, you can transfer your data sources from your current Receiver to the new one.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the Receiver, then click the **Properties** icon ⚙.

3 Click **Data Sources**.

4 Select the data sources to be migrated, then click **Migrate**.

5 Select the new Receiver in the **Destination Receiver** field, then click **OK**.

Import a list of data sources

Import a list of data sources (in .csv format), which eliminates the need to add, edit, or remove each data source individually.

You use this option in the following situations:

- To import raw data source data copied from a Receiver in a secured location to a Receiver in an unsecured location.
- 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

1 Export a list of 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**.

d Access and open this file.

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

a In column A, specify whether to add, edit, or remove the data source.

b If adding or editing data sources, enter the information in the spreadsheet columns.

You cannot 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.

c To import the changes, click **OK**.

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.

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.

j Click **OK**.

How vulnerability assessment works

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

You can use VA 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.
- Change Policy Editor configuration, such as turn on MySQL signatures if an asset is discovered running MySQL.

Use predefined or custom views to access VA data generated by the system.

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.

McAfee maintains rules that map McAfee sigIDs to VINs to references to a Common Vulnerabilities and Exposure (CVE) ID, BugTraq ID, Open Source Vulnerability Database (OSVDB) ID, or Secunia ID. These vendors report CVE and BugTraq IDs in their vulnerabilities.

Obtain McAfee Vulnerability Manager credentials

To connect McAfee Vulnerability Manager to McAfee ESM, you must obtain McAfee Vulnerability Manager credentials (such as the certificate and passphrase).

Task

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.

Run McAfee Vulnerability Manager scans

Set up McAfee ESM to run McAfee Vulnerability Manager vulnerability scans. An API checks for logon credentials, and populates the scan list based on those credentials every 60 seconds.

Task

1. On the system navigation tree, select **MVM Properties**, then click **Scans**.
2. Click **New Scan** and enter the information requested.

Option	Definition
IP Address/Range	Enter the IP address, range, or URL to be scanned.
Scan Name	(Optional) Type a name for the scan. If you don't enter a name, the McAfee Vulnerability Manager uses the default name `QuickScan_nn` (nn = your name).
Template	(Optional) Select the scan template, which is the name of an existing scan configuration. If you don't select one, the default is used.
Engine	(Optional) Select the scan engine. If you don't select one, the default is used.

3. Click **OK**.

Define VA system profiles for eEye REM

Define vulnerability assessment (VA) profiles to use adding an eEye REM source.

Task

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**.

Qualys QualysGuard log files are limited to 2 GB.

Add VA sources

To communicate with vulnerability assessment (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

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.

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 you leave this field blank, the system scans all companies to which the user belongs. Separate multiple company names with commas.
Data Retrieval	(Qualys QualysGuard) Select the method to retrieve the VA data. **HTTP/HTTPS** is the default. Options include: **SCP**, **FTP**, **NFS**, **CIFS**, and **Manual upload**. A Qualys QualysGuard log file manual upload has a file size limit of 2 GB.
Domain	Type the domain of the Windows system (optional, unless your domain controller or server exists in a domain).
Exported scan file directory	Directory where exported scan files reside
Exported scan file format	Exported scan file format (XML, NBE)
Install directory	Location where Saint was installed on the server. The installation directory for a Saint appliance scanner is `/usr/local/sm/`
IP Address	• For eEye REM: IP address of the eEye server that sends trap information • For eEye Retina: IP address of the client holding exported scan files (.rtd) • For Nessus, OpenVAS, LanGuard, and Rapid7 Metasploit Pro: IP address of the client holding exported scan files • For NGS: IP address of the system storing the Squirrel reports • For Rapid7, Lumension, nCircle, and Saint: IP address of the respective server

Option	Definition
Mount Directory	If you select **nfs** in the **Method** field, the system adds **Mount Directory** fields. Enter the mount directory set when you configured **nfs**.
Method	Method used to retrieve exported scan files (**SCP**, **FTP**, **NFS**, or **CIFS** mount). LanGuard always uses **CIFS**.
Password	• For Nessus, OpenVAS, LanGuard, and Rapid7 Metasploit Pro: The password of SCP or FTP. • For NGS: The password for the SCP and FTP methods. • For Qualys and FusionVM: The password for the Qualys Front Office or FusionVM user name. • For Rapid7 Nexpose, Lumension, nCircle, and Saint: The password to use when connecting to the web server. • For Digital Defense Frontline: The web interface password.
Port	The port Rapid7 Nexpose, Lumension, nCircle, or Saint web server are listening on. The default for Rapid7 Nexpose is 3780, for Lumension is 205, for nCircle is 443, 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	IP address of the HTTP proxy
Proxy Password	Password for the proxy user name
Proxy Port	Port on which the HTTP proxy is listening
Proxy Username	User name for the proxy
Qualys or FusionVM server URL	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**	Indicate the frequency to retrieve VA data from the Receiver or DEM: • **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. If you do not want the data retrieved at a preset time, select **Disabled**. eEye REM does not support data retrieval from the source so the data must be retrieved from the Receiver or DEM.
Schedule VA data retrieval	Indicate the frequency to retrieve VA data from the VA source.
Session	Saint: The session data is gathered from. To include all sessions, type **All**.

Option	Definition
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.
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 see the same protocol type). Make sure that your REM Events Server configuration matches your selection.
SNMP Community	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	Security level for this source: • **noAuthNoPriv** — No authentication protocol and no privacy protocol • **authNoPriv** — Authentication protocol but no privacy protocol • **authPriv** — Both authentication and privacy protocol. 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.
SNMP user name	Security name in **REM Events Server Configuration**
SNMP version	Version of SNMP for the source. The SNMP fields are activated based on the version you select.
SNMPv3 Engine ID	(Optional) The SNMPv3 Engine ID of the trap sender, if you use an SNMPv3 profile.
Sudo password	(Optional) Type the password that is required to access the Saint installation directory.
Time out	Allows you to use the default time-out value for a source or provide a specific time-out value. 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	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. 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.
Use System Profile (eEye REM)	Select whether to use a previously defined profile. This option deactivates all SNMP fields. When you select one of the existing system profiles, the system populates fields with the information in the selected profile.

Option	Definition
User name	If you use Windows authentication mode for the SQL Server, enter the user name of the Windows box. If not, enter the user name of the SQL Server. • For Nessus, OpenVAS, and Rapid7 Metasploit Pro: User name of SCP or FTP • For NGS: User name for the SCP and FTP methods • For Qualys or FusionVM: Front Office or FusionVM user name with which to authenticate • For Rapid7 Nexpose, Lumension, nCircle, and Saint: User name when connecting to the web server • For Digital Defense Frontline: Web interface user name
VA Source Name	Name for this source
Wildcard expression	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, 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.

4 Click **Apply** or **OK**.

Retrieve VA data

You can retrieve scheduled or immediate vulnerability assessment (VA) data from a data source. eEye REM data retrieval cannot be immediate; it must be scheduled.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, select the DEM or the **Receiver**, then click the **Properties** icon ⚙.

3 Click **Vulnerability Assessment**.

4 Select the VA source, then select one of these options:

- To retrieve immediately, click **Retrieve**. The job runs in the background and you are informed if the retrieval is successful.
- To schedule retrieval, click **Edit**. Select the frequency then choose to write the changes to the device.

5 Click **OK**.

6 If you cannot retrieve VA data, check the following:

This resource...	Causes...
Nessus, OpenVAS, and Rapid7 Metasploit Pro	• 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; so, 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 the FTP site before uploading the new one, or use a different name for the file you upload.

7 To view the data, click the **Asset Manager** icon , then select the **Vulnerability Assessment** tab.

How SNMP and MIB work

Configure settings to send link up and down and cold and warm start traps, from McAfee ESM and each device. Retrieve Management Information Base (MIB)-II system and interface tables, and allow discovery of McAfee 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 McAfee ESM for McAfee ESM and McAfee Event Receiver, health information. SNMPv3 traps can be sent to McAfee ESM to add to the blacklist of one or more of its managed devices. You can also configure all devices to send link traps and boot traps to destinations of your choosing.

SNMP and the McAfee MIB

McAfee products 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** — McAfee 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 aN SNMP data source.
- **McAfee ESM Health Requests** —McAfee ESM can receive and respond to health requests for itself and the devices it manages.
- **Blacklist** — McAfee 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, McAfee ESM). The devices typically perform an SNMP `GET` request by providing the host name of McAfee ESM and OIDs, with the specific instance of the OID.

McAfee ESM responds by populating the OID bindings with the results of the health request.

The following tables show the meaning of McAfee ESM and Receiver OIDs.

Table 9-13 McAfee 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 McAfee ESM database
1.3.6.1.4.1.23128.1.3.1.5	MB	1363148	Free HDD space available for McAfee 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 McAfee ESM
1.3.6.1.4.1.23128.1.3.1.7		8.4.2	McAfee ESM version and buildstamp
1.3.6.1.4.1.23128.1.3.1.8		4EEE:6669	Machine ID of the McAfee ESM
1.3.6.1.4.1.23128.1.3.1.9		McAfee ESM	McAfee ESM model number

Table 9-14 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	McAfee 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 9-14 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 McAfee 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	McAfee 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	0:0:0:0:0:0:0:0	IPv6 source IP address
1.3.6.1.4.1.23128.1.1.25	0:0:0:0:0:0:0:0	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

How SNMP traps work with data sources

SNMP traps allow data sources to accept standard SNMP traps from any manageable network device capable of sending SNMP traps.

Standard SNMP traps include:

- 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:

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

Configure SNMP settings

Define the settings for inbound and outbound SNMP traffic. Only users without spaces in their user names can perform SNMP queries.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **SNMP Configuration**.

3 Enter the required information then click **OK**.

Tab	Option	Definition
SNMP Requests	**Request Port**	Select the port where the traffic passes.
	Accept	Select which trap types 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 McAfee ESM allows. 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**	Set the port where the cold/warm trap traffic and the blacklist entry and link up/link down traffic passes.
	Link Up/Down Traps	Select to send Link Up and Link Down traps. If selected and you use multiple interfaces, the system notifies you when an interface goes down or comes back up. The system allows cold/warm trap traffic automatically. Cold start traps generate any time the SNMP service restarts. The SNMP service can restart after you make SNMP configuration changes, change users or groups, users log on with remote authentication, or the McAfee ESM reboots, cpservice restarts. Restarting the system generates a warm start trap.
	Database Up/Down Traps	Select to send SNMP traps when the database (cpservice, IPSDBServer) goes up or down.
	Security Log Failure Trap	Select to send SNMP traps when the system does not write logs to the log table.
	General Hardware Failure	To avoid a shutdown due to power failure, select to be notified when power supplies fail for general hardware or DAS.
	Destinations	Select the system profile names you want to receive notifications.

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 privileges 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).

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **SNMP Configuration**, then click the **SNMP Traps** tab.
4. In **Trap Port**, type `162`, then select **General Hardware Failure**, and click **Edit Profiles**.
5. 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.
6. Click **OK**, then click **Close** on the **Profile Manager** page.

   The profile is added to the **Destinations** table.
7. 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.

Configure SNMP notifications

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

If you set up SNMP on a high availability (HA) Receiver, the traps for the primary Receiver go out through the shared IP address. So, when you set up the listeners, set one up for the shared IP address.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **SNMP Configuration**.

4 Select the **SNMP Requests** tab and configure the settings.

Table 9-15 Option definitions

Option	Definition
SNMP Requests	**Request Port**
Accept	Sets the requests to be accepted.
Allow SNMPv1	Allows SNMP version 1 and version 2 traffic, and set the community string.
Allow SNMPv3	Allows SNMP version 3 traffic, and select the security level, authentication protocol, and privacy protocol.
Trusted IP Addresses	Shows 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.

5 Select the **SNMP Traps** tab and configure the settings.

Option	Definition
Trap Port	Sets the port where the cold/warm trap traffic, blacklist entry, and link up/link down traffic passes.
Link Up/Down Traps	Sends 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	Sends an SNMP trap when the database (cpservice, IPSDBServer) goes up or down.
Security Log Failure Trap	Sends an SNMP trap when a log is not written to the log table.
Destinations	Sets the profile names of the systems where you want the notifications sent. The table shows all available SNMP trap profiles on the system. You can edit this list by clicking **Edit Profiles**.

Pull the MIB from McAfee ESM

View the objects and notifications for interfacing with McAfee ESM.

The objects and notifications defined in this MIB are used to send requests:

- To a McAfee ESM requesting health status information for the McAfee ESM itself or for Receiver devices
- To a device to request its health status information.

Task

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

2 Select the **SNMP Requests** tab, then click **View MIB**.

General device settings

Contents

Find device-specific details

Use this information when you need to know device characteristics. For example, Technical Support might ask for this information during troubleshooting.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 To refresh device status, click ↻ on the system navigation tree.

3 On the system navigation tree, select the device, then click the **Properties** icon ⚙.

Device-specific information appears:

Option	Definition
Machine ID	Device identification number. To reactivate your system, McAfee Support uses 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	Syncs the clock on this device to the clock on McAfee ESM
Zone	Zone the device has been assigned to, if one has been assigned. If you click **Zone**, **Zone Policy Manager** opens.
Policy	Current state of the policy on this device. If you click **Policy**, the **Policy Editor** opens.
Status	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)

4 To view device performance statistics, logs, and network interface statistics, click **<device> Management**, then click **View Statistics**.

Install SSL certificate

McAfee ESM ships with a default self-signed security (SSL) certificate for esm.mcafee.local. Most web browsers cannot warn they cannot verify the certificate's authenticity. Once you obtain the SSL key certificate pair for your McAfee ESM, you must install it.

Task

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. The system prompts you 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 McAfee ESM. • Click **Generate**, enter the information in **Manage Certificate**, then click **OK**. • Click **Generate**.
Signed Certificate Request	Generate a certificate request to send to a certificate authority for signature. • Click **Generate**, enter the information in **Manage Certificate**, 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.

Regenerate SSH key

Regenerate the private or public SSH key pair to communicate with all devices.

Task

1 On the system navigation tree, select **System Properties**, then click **ESM Management**.

2 On the **Key Management** tab, click **Regenerate SSH**.

3 Click **Yes**.

When the system regenerates a new key, it replaces the old key pair on all devices managed by McAfee ESM.

Manage multiple devices

Start, stop, and restart, or update the software on multiple devices at one time.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Configuration**.

2 On the system navigation tree, use Ctrl+click and Shift+click to select the devices you want to manage.

3 Click the **Multi-Device Management** icon on the actions toolbar.

4 Select the operation you want to perform and the devices you want to perform it on, then click **Start**.

Manage URLs for devices

You can set up a URL to open from links on the **Event Analysis** and **Flow Analysis** views of a device.

Before you begin

Make sure the URL is functional.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **Custom Settings** | **Device Links**.
4. On the Custom Device Links page, select the device, then click **Edit**.
5. Enter a URL (maximum of 512 characters).
6. If the URL includes the address of a third-party application and you need to append variables to the URL, click where you want the variable inserted, then click the variable icon and select the variable.
7. Access the information page by clicking the **Launch Device URL** icon 🌐 at the bottom of the **Event Analysis** and **Flow Analysis** views of a device.

Sync devices with McAfee ESM

If you have to replace McAfee 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 McAfee ESM so they can resume pulling events.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon ⚙.
3. Click **<device label> Configuration** | **Sync Device**.
4. When the sync is completed, click **OK**.

Start, stop, reboot, or refresh a device

These actions can be useful during maintenance or troubleshooting.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select the device, then click the **Properties** icon ⚙.
3. Select **<device> Information**.
4. Click **Start**, **Stop**, **Reboot**, or **Refresh**.

Stop automatic refresh of the McAfee ESM system tree

The McAfee ESM system tree refreshes automatically every 5 minutes. If needed, you can stop that automatic refresh.

Before you begin

Verify that you have **System Management** privileges to change this setting.

Task

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

During the refresh, you can't select devices on the tree.

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.

Define profiles for common information and remote commands

Share common information for syslog-based traffic, like event forwarding, data source configuration, network discovery, vulnerability assessment, SNMP traps, and remote share. Define profiles for syslog-based traffic so you can share common information. You can also add remote command profiles (URL or Script) for views or alarms.

Task

1 From the McAfee ESM dashboard, click and select **System Properties**. Then click **Profile Management**.

2 On the **System Profiles** tab, define the profile. Fields vary based on which **Profile Type** you select.

3 On the **Remote Command** tab, define a profile to execute for views or alarms. The scripts can reference variables from the queries or event.

Use remote command settings to execute commands on devices that accept SSH connections, exceptMcAfee ESM devices.

Delete duplicate device nodes

Duplicate device nodes can appear on the system navigation tree. To avoid confusion, delete duplicate device nodes.

Task

1 From the McAfee ESM dashboard, click and select **Configuration**.

2 In the system navigation pane, click the display type drop-down list.

3 Select the **Edit** icon next to the display that includes the duplicate devices.

4 Deselect one of the duplicate devices, then click **OK**.

Mask IP addresses

Mask IP addresses for event data sent out in event forwarding or to a primary McAfee ESM.

Task

1 From the McAfee ESM dashboard, click ☰ and select **System Properties**.

2 Click **ESM Management** | **ESM Hierarchy**.

3 To mask data, select **Obfuscate** for McAfee ESM devices.

4 Select the fields that you want to mask.

5 Select settings on your Local Network.

- To ensure obfuscation occurs 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 McAfee ESM devices and want to keep the values synchronized.
- Select to hide IP addresses inside and outside your local network. This extends to IP address custom types such as IPv4 and IPv6 addresses.
- Enter a list of the IP addresses or subnets included in your Local Network, separated by commas (maximum of 2,000 characters).

  If your Local Network is longer than 2,000 characters, consolidate multiple subnets into a shorter Local Network using Classless Inter-Domain Routing (CIDR) notation.

Once this is set up, if a primary McAfee ESM requests a packet from a secondary McAfee ESM, the system masks the data you selected.

Upgrade primary or redundant devices

Upgrade primary or redundant devices.

Task

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 device.

3 Update the redundant device.

4 Enable the collection of events, flows, and logs by selecting **Auto check every** once again.

Manage task queries

The Task Manager displays a list of the queries that are running on McAfee ESM. You can view their status and delete any that affect system performance.

Task

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

2 Click **ESM Management**, click the **Maintenance** tab, then click **Task Manager**.

3 You can do the following tasks:

- Close report, view, watchlist, execute and export, alarm, and external API queries on the system. You cannot close system queries.
- By default, the list refreshes automatically every 5 seconds. If you select a query and the list auto-refreshes, it remains selected but refreshes the details. Completed queries do not appear on the list.
- Select and copy the data in the **Query Details** area.
- Sort the table columns.
- ✕ identifies queries you can close.

Set system time

Contents

Set system time

The system time stamps activities generated by McAfee ESM and its devices. Select a system clock or NTP servers to ensure that the system uses a constant time reference for synchronize the time stamps.

Before you begin

If you intend to synchronize the system's time using NTP servers, verify that the servers exist and that you have their authorization keys and key IDs.

Task

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**.

Option	Definition
Set the ESM System Time (GMT) to	Select this option to set the system clock to Greenwich mean time (GMT) instead of synchronizing to NTP servers.
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.
NTP Server column	Add the IP addresses for NTP servers; 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.
Status	Click to view the status of the NTP servers on the list. If you change the list of servers, click **OK** to save the changes and close the page. Then reopen the page before clicking **Status**.

Synchronize device clocks

Synchronize device clocks with the McAfee ESM system time so that data generated by the various systems reflects the same time stamps.

Task

1 On the system navigation tree, select **System Properties** or device **Properties**, then click **Sync** in the **Sync Device Clock** field.

2 Click **Refresh** to update the data on **System Information** or device **Information**.

Set up Network Time Protocol (NTP)

Manage Network Time Protocol (NTP) servers for the device and indicate if you want to use NTP servers for time synchronization.

Task

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**.

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. NTP server addresses on IPS class 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 change the list of servers, you must click **OK** to save the changes and close the page, then open the page again before clicking **Status**.

View status of Network Time Protocol (NTP) servers

View the status of Network Time Protocol (NTP) servers on McAfee ESM.

Before you begin

Add NTP servers to McAfee ESM or devices.

It can take up to 10 minutes for changes to appear.

Task

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**.

Option	Definition
NTP Server column	Lists the IP addresses for the NTP servers. These markings might appear before the address: • * – 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** indicates no credentials exist • **bad** indicates incorrect credentials • **yes** indicates correct credentials
Condition column	The condition corresponds to the mark in the **NTP Server** column. • **candidate** indicates a possible choice • **sys.peer** indicates the current choice • **reject** indicates it can't be reached. If all servers are selected **reject**, it's possible that the NTP configuration is restarting.

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.

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** - an integer that identifies 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.

- **Device Vendor**, **Device Product**, and **Device Version** - strings that uniquely identify the type of sending device.

  No two products can use the same device-vendor and device-product pair. Event producers ensure that they assign unique name pairs.

- **DeviceEventClassId** - unique identifier per event-type (can be a string or an integer).

  DeviceEventClassId identifies the type of event reported. 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** - string describing the event, such as *Port scan*

- **Severity** - integer (between 0-10, where 10 indicates the most important event) that reflects event importance.
- **Extension** - collection of key-value pairs, where the keys are part of a predefined set.

  Events 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 on exactly that manner. For example: `fileName=c:\Program Files\ArcSight is a valid token.`

This sample message shows 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 looks 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*.

10 Managing assets

Contents

How the Asset Manager works

The *Asset Manager* provides a centralized location that allows you to discover, manually create, and import assets.

An *asset* is any device with an IP address added to McAfee ESM. The Asset Manager enables you to manage the assets on your network.

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 McAfee 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.

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.
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: `Hostname, IPAddress, Mask, ZoneName, UsrSeverity, UseCalcSeverity, TagCount, TagGroupName:TagName` Add one `TagGroupName:TagName` for each tag you have (`TagCount`). Each asset must be on its own line.
File | **Export to file**	Export the selected asset files.

Table 10-1 Main menu options *(continued)*

Option	Definition
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. 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.
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. If you select this option and you changed the rate in the **Criticality** field, the **Calculate** and **Groups** buttons are active.
Calculate	Calculates the overall severity, which is added to the **Calculate** field.

Table 10-3 New asset advanced settings *(continued)*

Option	Definition
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.

Define old assets

The **Old Assets** group on the **Asset Manager** allows you to store assets that haven't been detected in a specified time.

Task

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**.

Manage asset sources

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, which 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. 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, change the `networkAddress` attribute on your computer objects so the system uses those IP addresses instead of querying DNS.

Before you begin

To retrieve assets on Altiris, you must have **Asset Manager** privileges on the Altiris Management Console.

Task

1 Click the **Asset Manager** quick launch icon, then click the **Asset Sources** tab.

The **Asset Sources** tree shows the McAfee ESM devices and Receivers on the system, and their current asset sources.

McAfee ESM can have one and Receivers can have multiple asset sources.

2 Select a device then select either of the available actions.

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 is retrieved at the 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.

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

1 From the dashboard, click ☰ and select **Asset Manager**.

2 Select the **Threat Management** tab.

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**.

Manage vulnerability assessment sources

Vulnerability assessment sources allow you to communicate with and retrieve data from VA vendors.

Task

1 From the dashboard, click ☰ and select **Asset Manager**.

2 Select the **Vulnerability Assessment** tab.

3 Add, edit, remove, or retrieve VA sources, then write them to the device.

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 you enter more than 1 company, 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**. A Qualys QualysGuard log file manual upload has a file size limit of 2 GB.
Domain	Type the domain of the Windows box (optional, unless your domain controller or server exists in 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 /usr/local/sm/.
IP Address	• eEye REM: The IP address of the eEye server that is sending trap information. • eEye Retina: The IP address of the client holding exported scan files (.rtd). • McAfee® Vulnerability Manager: The IP address of the server on which it is installed. • Nessus, OpenVAS, LanGuard, and Rapid7 Metasploit Pro: The IP address of the client holding exported scan files. • NGS: The IP address of the system that is storing the Squirrel reports. • 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**.

Option	Definition
Password	• 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. • Nessus, OpenVAS, LanGuard, and Rapid7 Metasploit Pro: The password of SCP or FTP. • NGS: The password for the SCP and FTP methods. • Qualys and FusionVM: The password for the Qualys Front Office or FusionVM user name. • Rapid7 Nexpose, Lumension, nCircle, and Saint: The password to use when connecting to the web server. • Digital Defense Frontline: The web interface password.
Port	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	IP address of the HTTP proxy.
Proxy Password	Password for the proxy user name.
Proxy Port	Port on which the HTTP proxy is listening.
Proxy Username	User name for the proxy.
Qualys or FusionVM server URL	URL of the Qualys or FusionVM server to query.
Remote path and share name	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**	Indicate the frequency with which you want the VA data to be retrieved from the Receiver or DEM: • **Daily** — time to retrieve data each day. • **Weekly** — Day of the week and the time on that day to retrieve data. • **Monthly** — Day of the month and the time on that day to retrieve data. If you do not want to retrieve data at a preset time, select **Disabled**. eEye REM does not support data retrieval from the source so the data must be retrieved from the Receiver or DEM.
Schedule VA data retrieval	Indicate the frequency with which you want the VA data to be retrieved from the VA source.
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.
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 see the same protocol type). Make sure that your REM Events Server configuration matches your selection.
SNMP Community	SNMP community set when you configured the REM Events Server.

Option	Definition
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	Security level you want to set for this source. • **noAuthNoPriv** — No authentication protocol and no privacy protocol • **authNoPriv** — Authentication protocol but no privacy protocol • **authPriv** — Both authentication and privacy protocol. 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.
SNMP user name	Security name in **REM Events Server Configuration**.
SNMP version	Version of SNMP for the source. The SNMP fields are activated based on the version selected.
SNMPv3 Engine ID	(Optional) 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.
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. 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.
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.
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. • Nessus, OpenVAS, and Rapid7 Metasploit Pro: The user name of SCP or FTP. • NGS: The user name for the SCP and FTP methods. • Qualys or FusionVM: The Front Office or FusionVM user name with which to authenticate. • Rapid7 Nexpose, Lumension, nCircle, and Saint: The user name to use when connecting to the web server. • Digital Defense Frontline: The web interface user name.

Option	Definition
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.

Zone Management

Use *zones* 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, add two zones. Then, assign the devices whose events must be grouped to each of the zones. To group the events from each office by specific IP addresses, add subzones to each of the zones.

Manage zones

Zones categorize your devices and data sources by geolocation or ASN. Add zones, either individually or by importing a file exported from another system. Then assign the devices or data sources to the zones.

Task

1. From the dashboard, click ☰ and select **Asset Manager**.
2. Select the **Zones Management** tab.
3. Add a zone or subzone, edit or remove existing zones, or import or export zone settings.
4. Roll out changes, then click **OK**

Add zones

Add zones individually using the **Add Zone** feature or import a file exported from another system.

Task

1. From the dashboard, click ☰ and select **Asset Manager**.
2. Select the **Zone Management** tab.
3. Click **Add Zone**.

4 Enter the information requested and assign devices to the zone, then click **OK.**

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 subzones.
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.

5 To add subzones to a zone, select the relevant zone and click **Add Sub-Zone**. Enter the details for the subzone, such as name, description, IP address range, and geolocation or ASN information.

Export zone settings

Export zone settings from one McAfee ESM and import them to another McAfee ESM.

Task

1 From the dashboard, click ☰ and select **Asset Manager**.

2 Select the **Zone Management** tab.

3 Click **Export**, then select the type of file you want to export:

- **Export zone definition file** - includes settings for zones and their corresponding subzones
- **Export device to zone assignment file** - includes devices and zones assigned to those devices

4 Click **OK** and select the file to download.

Import zone settings

Import zone settings from a file *as is* or edit the data before importing it.

Before you begin

Export a file of zone settings from one McAfee ESM so that it can be imported to another McAfee ESM.

Task

1 Open the zone settings file that you want to import.

- An import zone definition file contains 8 columns: Command, Zone Name, Parent Name, Geo Location, ASN, Default, IPStart, and IPStop.
- An import device to zone assignment file contains 3 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 changes made to the data.

  To change a subzone range, remove the existing range, then add the range with the changes. You can't edit the subzone range directly.

- `remove` — Delete the zone matching this line from the McAfee ESM.

3 Save your changes and close the file.

4 From the dashboard, click ☰ and select **Asset Manager**.

5 Select the **Zone Management** tab.

6 Click **Import**, then select the import file type.

- **Import zone definition file** - includes settings for zones and their corresponding subzones
- **Import device to zone assignment file** - includes devices and zones assigned to those devices

7 Click **OK**, then locate the file to be imported and click **Upload**.

The system indicates detected errors in the file.

8 If there are errors, correct the information and try again.

9 Roll out the changes to update the devices.

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.

Asset, threat, and risk assessment

McAfee Threat Intelligence Services (MTIS) and the vulnerability assessment sources on your system generate a list of known threats. McAfee ESM uses the threat severity and the criticality of each of your assets to calculate the level of risk to your enterprise.

Asset Manager

When you add an asset to your **Asset Manager**, you assign a criticality level that 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 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 and countermeasures you can use.

Predefined views

Predefined 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.

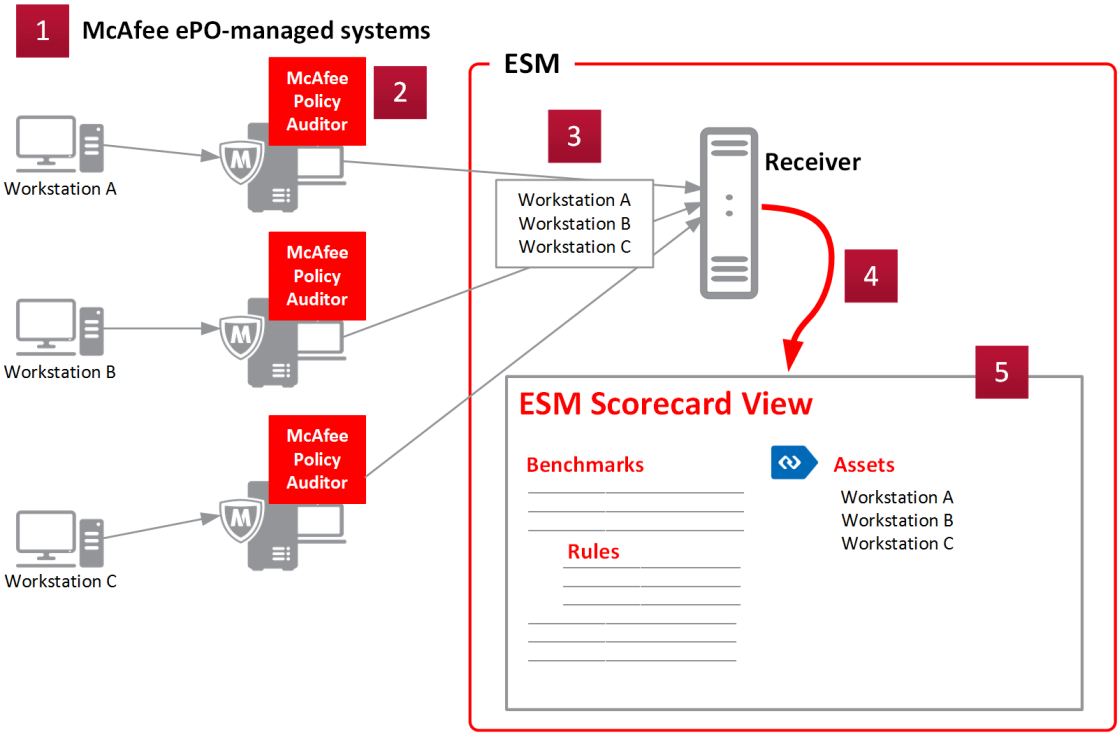
Custom views

Use the **Query Wizard** to set up custom views 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.

How the Scorecard works

The McAfee ESM *Scorecard* shows which assets (endpoints) meet your organization's configuration requirements (benchmarks).



1 Configure McAfee ePO with McAfee Policy Auditor to audit your system assets (endpoints).

2 Benchmarks contain rules that determine whether assets meet required configurations. McAfee Policy Auditor defines which benchmarks and frequency to use to audit assets.

McAfee Policy Auditor feeds audit results to McAfee ePO.

3 The McAfee Event Receiver pulls audit results from McAfee ePO.

4 The McAfee Event Receiver shares audit data with McAfee ESM.

5 The McAfee ESM Scorecard shows:

- Executive summaries of your organization's assets (endpoints) and benchmark results
- Scorecard data filtered by specific assets or benchmark result data
- Percentage of benchmarks that assets passed
- Statistics for the average benchmark score
- How many assets the score represents
- Trends over time

  Trend lines appear only if at least two data points exist, which is about two weeks of data.

- How assets and benchmarks are bound

Configure the Scorecard

Define what data appears on the Scorecard.

Before you begin
Confirm that McAfee ePO is installed with McAfee Policy Auditor running.

Task

1 From the McAfee ESM dashboard, click ☰ and select **Scorecard**.

2 Choose the assets and benchmarks you want to appear in the Scorecard.

a On the **Benchmark Groups** or **Asset Groups** pane, click ⋮.

b Click **Settings**, then select what you want to display.

When selecting Scorecard data, consider the volume of data and its effect on performance. Benchmarks contain sets of rules and display one data point for multiple rules. Rules can display large amounts of data.

3 Define how data appears on the Scorecard:

- To calculate trends over time, choose a period between 1 week and 12 months.

  Use short periods to identify highly volatile trends. Use longer periods to identify deviations from standard benchmarks.

- To toggle the binding direction between assets and benchmarks, click  .

  By default, benchmark data is bound to assets.

- To toggle between text view and graph view, click either the hash or bar chart icon.
- To drill down to a specific rule or asset, click the arrow next to the group name.
- To view data for a particular rule, group, or asset, select it.

  Data for only the selected rule, group, or asset appears in the bound table.

Configure executive Scorecard views

Define what you want to see in a visual summary of your organization's assets or benchmarks.

Before you begin

Confirm that McAfee ePO is installed with McAfee Policy Auditor running.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Scorecard**.
2. From the **Scorecard View** drop-down, choose the **Executive View** by benchmark or by asset.
3. Click ⚙ to choose which groups to display on that view.

   ℹ You can display a maximum of 12 groups.
4. Specify severity thresholds to show rule compliance levels in the view.

Filter Scorecard data

Filter Scorecard data to show only the asset or benchmark details that you want to see.

Before you begin

Confirm that McAfee ePO is installed with McAfee Policy Auditor running.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Scorecard**.
2. Click the filter bar and add fields or values by which you want to filter.

   The filter bar supports the following operators:
   and, equal, not equal, contains, not contains
3. Click 🔍.
4. To refresh the view data, click ↻.
5. To remove the filter and refresh the data, select **Clear & refresh**.

Report on Scorecard data

Export Scorecard data to a CSV file, which you can then use to report on your organization's benchmarks and assets.

Before you begin

Confirm that audit results have been pulled into the Scorecard from McAfee ePO with McAfee Policy Auditor.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Scorecard**.
2. Filter the Scorecard data, as needed.

The system generates a CSV file with the data associated with the selected group and applied filters.

- To filter by specific fields or values, use the filter bar.
- To show data for a specific group, right-click that benchmark or asset group.
- To show events related to a particular asset, right-click on a specific asset and choose the **Summarize by** option.

3 Click **Export**.

4 Format the CSV file to reflect your reporting needs.

11 Defining policies and rules

Contents

How McAfee ESM policies and rules work

Policies enable you to detect malicious or anomalous traffic and variables that act as parameters for *rules*. To guide the behavior of McAfee ESM devices, use the **Policy Editor** to create policy templates and customize individual policies.

Policy templates and device policy settings can inherit values from their parents. *Inheritance* allows device policy settings to be infinitely configurable while maintaining a level of simplicity and ease-of use. Each policy when created adds an entry to the **Policy Tree**.

When operating in FIPS mode, do not update rules through the rule server. Instead, update them manually.

Icon	Description
	Policy
	Out-of-sync device
	Staged device
	Up-to-date device

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.

Rule types listed in the **Policy Editor** vary based by the selected device in the system navigation tree. The system displays the policy hierarchy for the selected device. You can filter rules to view only those rules that meet your criteria. Or tag rules to define their functions.

Manage policies

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 privileges.

Task

1 From the dashboard, click ☰ and select **Policy Editor**.

2 On the McAfee ESM console, click the **Policy Editor** icon , then click the **Policy Tree** icon .

3 Use the **Policy Tree** to:

- See rules associated with policies
- Create a policy hierarchy

  You can only drag and drop devices onto policies.

- Search for policies or devices using filters or tags
- Rename, delete, copy, or replace policies

  Copied policy settings are applied to replaced policies, but the name remains the same.

- Move policies to different devices
- Import policies

  If importing multiple policies, the first policy overwrites the selected policy and the system inserts subsequent policies as children of the current node, leaving their hierarchical relationship intact. This option doesn't change the name of the selected policy.

- Export policies

  - Due to the possible dependency of custom rules on custom variables, you cannot export custom rules without also exporting the custom variables.
  - Policy hierarchy is flattened, which means the system compresses settings into one level of policy, with the most immediate policy's settings taking precedence on an item by item basis. For example, if you select a device, the system exports both policies above the selected policy. To export a parent policy, you must select its child. Also, policy settings have precedence over the parent policy settings when the file is compressed down into one level of policy.

Set up database audit trails

Set up an audit trail to track access and changes made to the database or to tables associated with specific database events. The McAfee ESM compliance report lists audit trails associated with each event.

Before you begin

To generate audit trail events, you must add:

- Data Access rules
- Privileged User Audit Trails report

Task

1. From the dashboard, click ☰ and select **Policy Editor**.
2. In the **Rule Types** pane, select **DEM** | **Data Access**.
3. Highlight **DEM - Template Rule - Trusted Use Access From IP Range**.
4. Click **Edit** | **Copy**, then click **Edit** | **Paste**.
5. Change the name and properties of the new rule.
   a. Highlight the rule, then select **Edit** | **Modify**.
   b. Name the rule, then type the user name.
   c. Select the **Untrusted** action type, then click **OK**.
6. Click the **Rollout** icon .
7. 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**.
8. To generate the report, click **Run Now**.

How variables work

A *variable* is a global setting or a placeholder for information that is user- or site-specific and used by rules.

Adding or changing variables requires extensive knowledge of Snort format.

Use variables to make rules behave in specific ways, which might vary from device to device. McAfee ESM has many pre-set variables, but also allows you 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; set some values that correspond to the specific environment of each device. Variable names cannot contain spaces; Use an underscore (_) to represent spaces. To maximize device effectiveness, 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_SERVE RS	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

You can change system variables and add, change, or delete custom variables.

Assign types to custom variables to filter rules for reporting. Types determine the field in which the variables are available when adding or changing a rule. Variable types are global, and changes appear on all policy levels.

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

1 Click the **Policy Editor** icon.

2 On the **Rule Types** pane, select **Variable**.

3 Do any of the following:

- Add a category by selecting **New** | **Category**.
- Add custom variables by selecting the category, then click **New**, then select **Variable**, then define the requested settings.
- Change variables by selecting the variable, then select **Edit**, then click **Modify** or **Delete**.

  When the variable type is set to something other than **No Type Selected** and committed, you can't change the value.

- Import variables by selecting **File**, then click **Import** | **Variables**. Click **Import**, then browse and upload the file.

  The import file must be a .txt file with the following information in this format: VariableName;VariableValue; CategoryName (optional); Description (optional). If one field is missing, a semicolon must be in place to act as a place holder.

4 In the rules display pane, select the category, then click **New**.

5 Select **Variable**, then define the requested settings.

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

1. On the McAfee ESM console, click the **Policy Editor** icon .
2. In the **Rule Types** pane, click **Variable**.
3. In the Variables pane, expand the **preprocessor** group, then double-click **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**.

McAfee ESM rule types

McAfee ESM includes many types of rules that enable you to protect your environment.

- McAfee Application Data Monitor rules -detect malicious traffic patterns by detecting anomalies in application and transport protocols.
- Advanced Syslog Parser (ASP) rules - identify where data resides in message-specific events, such as signature IDs, IP addresses, ports, user names, and actions.
- Correlation rules - interpret patterns in correlated data.
- Data source rules - detect issues with data source information sent to receivers.
- McAfee Database Event Monitor rules - monitor database events, such as logon/logoff, DBA-type activity, suspicious activity, and database attacks that are typically required to achieve compliance requirements.
- McAfee ESM rules - generate compliance or auditing reports related to McAfee ESM events.
- Filter rules - allow you to specify what action to take on McAfee Event Receiver data.
- Transaction tracking rules - track database transactions and auto-reconcile changes, such as log start and end of a trade execution or begin and commit statements to report by transactions instead of queries.
- Windows events rules - generate events that are related to Windows.

Icons indicate where a rule inherits its usage.

Icon	Description
	Indicates default setting inherits parent's use
	Indicates broken inheritance chain at this level. Inheritance turned off at this point. The current rule usage is used when the inheritance chain is broken.
	Indicates broken inheritance chain at this level. Items below this point do not inherit any further up the chain.
	Indicates a custom value; set the value to something other than the default.

McAfee Application Data Monitor rules

McAfee Application Data Monitor 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 can identify protocols and content types automatically without relying on fixed TCP port numbers or file extensions. ICE engine does not rely on signatures to perform analysis and decoding, instead its modules implement full parsers for each protocol or content type, which results in accurate identification and decoding of content and allows content to be identified and extracted even when that content is compressed or otherwise encoded. So, doesn't pass over the network in clear text.

As a result of this highly accurate identification and decoding, the ICE engine offers 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 McAfee Application Data Monitor to provide invaluable security context. It can detect threats not easily detected by traditional IDS or IPS, such as:

- Leak of sensitive information and documents or communication policy violations
- Unauthorized application traffic (for example, who is 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)

McAfee Application Data Monitor 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

McAfee Application Data Monitor can monitor applications and protocols (such as those listed below) and then decode and detect anomalies.

- 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 — such as AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook 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

- *Object* — 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 might contain additional objects such as images. A .zip file and each file in the .zip file are all objects. McAfee Application Data Monitor unpacks the container and treats each object inside as its own object.
- *Transaction* — a wrapper around the transfer of an object (content). A transaction contains at least one object; but, if that object is a container, like a .zip file, the single transaction might contain several objects.
- *Flow* — the TCP or UDP network connection. A flow might contain many transactions.

Manage custom rules

Use predefined rules as templates to create custom rules.

Task

- From **Policy Editor**, do any of the following:
  - View existing custom rules:
    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**.
  - Copy and paste rules.
  - Change custom rules.
  - Delete custom rules.

Add custom rules

Use logical and regular expressions to add custom McAfee Application Data Monitor, database, or correlation rules.

Task

1. From the dashboard, click ☰ and select **Policy Editor**.
2. Click **New**, then select the rule type you want to add.

3 Define database rules:

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 to which the rule belongs.
Type	Select the rule type.
Default Action	Select the alert action this rule triggers.
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 the rule's description, which then appears in the **Policy Editor**.

4 Define correlation rules:

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 to group events when they come into the correlation engine.
Correlation Logic area	Drag and drop logical elements and components in this are to set the rule's logic.
Parameters	Customize instances of a rule and component reuse.
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 rule description that appears in the **Policy Editor**.

5 Define fields and values that events must match to trigger a correlation rule:

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. • **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.

Option	Definition
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.

6 Define expression component settings:

Option	Definition
Not	Select to exclude the values you select.
Term	Select the metric reference for this expression.
Description	Type a description of the component.
Dictionary	If you want this rule to reference a McAfee Application Data Monitor dictionary that is on McAfee ESM, select it on the drop-down list.
Operator	Select the relational operator. McAfee Application Data Monitor • Equal to = • Not equal to != • Greater than >>= • Less than <= • Less than < McAfee Database Event Monitor Database • 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 values match the pattern.
Value	Select the variables to filter by. • 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. Enter the value to filter by.
Valid Input	View hints for the values that you can enter in the **Value** field.

Edit logical elements

You can change the default settings for the AND, OR, and SET logical elements.

Task

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**.

McAfee® Application Data Monitor rules syntax

McAfee Application Data Monitor rules provide a set of literals (numbers, strings, regular expressions, IP addresses, MAC addresses, and Booleans), similar to C expressions.

You can compare string terms with string and Regex literals to test their content but they can also be compared with numbers to test their length. You can only compare numeric, IP address, and MAC address terms 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 11-1 Operators

Operator	Description	Example
&&	Logical AND	protocol = = http && type = = image/gif
||	Logical OR	time.hour < 8 || time.hour > 18
^ ^	Logical XOR	email.from = = "a@b.com" ^^email.to = = "a@b.com"
!	Unary NOT	! (protocol = = http | | protocol = = ftp)
= =	Equal	type = = application/pdf
! =	Not equal	srcip ! = 192.168.0.0/16
>	Greater	objectsize > 100M
> =	Greater or equal	time.weekday > = 1
<	Less	objectsize < 10K
< =	Less or equal	time.hour < = 6

Table 11-2 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 11-3 Type operator compatibility

Type	Operators	Notes
Number	= =, ! =, >, > =, <, < =	
String	= =, ! =	Compare content of string with String/Regex
String	>, > =, <, <=	Compare length of string
IPv4	= =, ! =	
MAC	= =, ! =	
Bool	= =, ! =	Compare against true/false, also supports implied comparison with true, for example the following tests whether the email.bcc term occurs: email.bcc

Table 11-4 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

Escapes	
\x00	Hex Representation
\0000	Octal Representation
^	Start of line
S	End of line
	The start of line and end of line anchors (^ and $) don't work for objcontent.

POSIX character classes	
[:alunum:]	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

McAfee Application Data Monitor dictionary examples

McAfee Application Data Monitor can match object content or other metrics or properties with a single column dictionary for true or false (exists in the dictionary or does not exist in the dictionary).

Table 11-5 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 with 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 11-6 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 with 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 and 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”

McAfee® Application Data Monitor rule term types

McAfee Application Data Monitor rules contain terms that can be IP addresses, MAC addresses, numbers, strings, or a Boolean.

In addition, there are two extra literal types: regular expressions and lists. A term of a specific type can 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 ...).

Exceptions to this rule are:

- 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
- A string term can be compared against a regular expression. The following rule triggers if a password only contains lowercase letters: Password == /^[a-z]+$/
- 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	• 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	• MAC address literals are written using standard notation, as with IP addresses, they are not enclosed in quotes: aa:bb:cc:dd:ee:ff
Numbers	• All numbers in McAfee Application Data Monitor 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	• 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, the following rule does not trigger: email.from == “@somewhere.com” • To match only a part of a term, use a regular expression literal instead. String literals must be used when possible because they are more efficient.  All email address and URL terms are normalized before matching so it is not needed to take account of things like comments in email addresses.
Booleans	• The Boolean literals are true and false.

Type	Format description
Regular expressions	• Regular expression literals use the same notation as languages like JavaScript and Perl, enclosing the regular expression in forward slashes: /[a-z]+/ • Follow regular expressions with standard modifier flags, though "i" is the only one currently recognized (case-insensitive): /[a-z]+/i • Use the POSIX Extended syntax for regular expression literals. 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 in the term unless anchor operators are applied in the regular expression. The following rule triggers if an email is seen with an address of “someone@somewhere.com”: email.from == /@somewhere.com/
Lists	• List literals consist of one or more literals enclosed in square brackets and separated by commas: [1, 2, 3, 4, 5] • Lists might contain any kind of literal, including other lists: [192.168.1.1, [10.0.0.0/8, 172.16.128.0/24]] • Lists must only contain one 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 (!=), 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: Srcip == [192.168.1.1, 192.168.1.2, 192.168.1.3] • It is equivalent to: Srcip == 192.168.1.1 || srcip == 192.168.1.2 || srcip == 192.168.1.3 • When used with the not-equal (!=) operator, the expression is true if the term doesn't match all literals in the list. The following rule triggers if the source IP address is not 192.168.1.1 or 192.168.1.2: Srcip != [192.168.1.1, 192.168.1.2] • It is equivalent to: Srcip != 192.168.1.1 && srcip != 192.168.1.2 • Lists might also be used with the other relational operators, though it doesn't make much sense. The following rule triggers if the object size is greater than 100 or if the object size is greater than 200: objectsize > [100, 200] • It is equivalent to: objectsize > 100 || objectsize > 200

McAfee® Application Data Monitor rule metric references

Use the following metric references when adding McAfee Application Data Monitor rules.

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, but, be detected using Object Type (objtype)
Object Type (Number)	Specifies the type of the content as determined by McAfee Application Data Monitor (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)

Property or term	Description
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 address 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)

Protocol-specific properties

In addition to providing properties that are common across most protocols, McAfee Application Data Monitor also provides protocol-specific properties that can be used with McAfee Application Data Monitor rules.

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 11-7 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	Referrer		
	URL		
	All HTTP headers		

Table 11-8 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 11-9 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***

Protocol anomalies

Beyond the common properties and protocol-specific properties, McAfee® Application Data Monitor 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 a McAfee® Application Data Monitor rule.

Table 11-10 IP address

Term	Description
ip.too-small	IP address packet is too small to contain a valid header.
ip.bad-offset	IP address data offset goes past end of packet.
ip.fragmented	IP address packet is fragmented.
ip.bad-checksum	IP address packet checksum doesn't match data.
ip.bad-length	IP address packet totlen field goes past end of packet.

Table 11-11 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 is already 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 11-12 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.

Table 11-12 DNS *(continued)*

Term	Description
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.

Data source rules

Data source rules have defined default actions. The McAfee Event Receiver assigns it to the event subtype associated with the rule. The list of data source rules includes predefined and auto learned rules.

The McAfee Event Receiver auto learns data source rules as it processes the information sent to it by the data sources that are associated with the McAfee Event Receiver.

The **Data Source** option in the **Rule Types** pane is only visible when you select a policy, data source, **Advanced Syslog Parser**, or McAfee Event Receiver in the system navigation tree. The description area at the bottom of the page gives detailed information about the selected rule. All rules have a severity setting that dictates the priority associated with a rule, which impacts how the alerts generated for these rules are shown for reporting purposes.

Set data source rule actions

Set the value of the event subtype per data source rule, which means that you can set default rule actions for dashboards, reports, parsing rules, or alarms with different values, such as the outcome of a selective access rule (permit/deny).

Task

1. On the McAfee 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.

Manage auto-learned data source rules

View and change auto-learned data source rules.

Task

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 .
4. Select the rule you want to change 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**.

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.

Add filter rules

Add filter rules to the **Policy Editor**.

Before you begin
Verify that you have policy administrator privileges.

Task

1. On the **Policy Editor**, select **Receiver** | **Filter**.
2. Select **New**, then click **Filter Rule**.
3. Complete the fields, then click **OK**

Option	Definition
Tags	Click **Select** and choose tags to define the categories this rule belongs to.
Name	Type a name for the rule.
Normalized ID	(Optional) Click the **Normalized ID** icon, then select any additional normalized IDs.
Severity	(Optional) Change the severity setting for the rule.
Match All	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 is performed on all received data.
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 is performed. • To add a string, click **Add** and enter the string. • To edit or remove a string, select the string.
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 is performed.
Case Insensitive	Select if you want to add a case insensitive modifier so the PCRE content is matched regardless of the case.

Option	Definition
Action	Select the actions that are taken when the data received matches the PCRE and content strings, or on all 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, which appears in the **Description** field of the **Policy Editor** when the rule is selected.

4 To enable the rule, select the rule in the rule display pane, click the setting in the **Action** column, then click **enabled**.

Manage transaction tracking rules

Transaction tracking rules track database transactions and auto-reconcile changes, log start and end of a trade execution, or begin and commit statements to report by transactions instead of queries.

Task

1 On the **Policy Editor**, select **DEM** | **Transaction Tracking**.

2 Do one of the following:

- Click **New**, then click **Transaction Tracking Rule**.
- Select the rule on the rules display pane, then click **Edit** | **Modify**.

3 Fill in the information, then click **OK**.

Option	Definition
Type	Select the type of transaction tracking rule this is.
Rule Name	Type a name for the rule. It must be unique and can only contain alphanumeric characters, underscores (_), and spaces.
Start Query Tag	Type the SQL query to be executed before changing the database (for example, spChangeControlStart).
Stop Query Tag	Type the SQL query to be executed after changing 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.
Severity	Select the severity setting.
Description	Type a description of the rule.

Windows events rules

Windows events rules are used to generate events that are related to Windows.

They are data source rules for Windows events and are separated from the data source rule type because they are a common use case. McAfee defines these rules; you can't add, change, or delete them, but you can change their property settings.

Define packet oversubscription

Oversubscription defines how McAfee ESM handles packets if the device's capacity is exceeded. In each case, the packet is recorded as an event. 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.

Task

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**.

Changing **Oversubscription Mode** affects the primary and secondary devices (virtual devices). For this change to take effect, you must change the mode on the primary device.

View policy update status

Determine when to roll out policy updates by reviewing the policy update status for McAfee ESM devices.

Task

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**.

Working with rules

Contents

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 To view custom rules:

a Select the **Filter** tab in the **Filters/Tagging** pane.

b At the bottom of the pane, click the **Advanced** bar.

c If you want to view a Generic - Advanced Syslog Parser rule, clear the **Device Type ID** field.

d In the **Origin** field, select **user defined**, then click **Run Query** .

3 To copy and paste a rule:

a Select a predefined or custom rule.

b 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.

For ASP and Filter Rules, the rule order is copied as part of the copy process.

c Check that the ordering of the new rule will not adversely affect data parsing (**Operations** | **Order ASP Rules**) or (**Operations** | **Order Filter Rules**).

d To change the name, select **Edit** | **Modify**.

4 To modify a rule:

a Highlight the rule you want to view, then select **Edit** | **Modify**.

b 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**.

If you did not change the name of the rule, it is saved with the same name and a different sigID.

c You can change the name by selecting the rule, then selecting **Edit** | **Modify**.

Import rules

Import a set of rules from one McAfee ESM to another.

Task

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 can't be undone.

3 Click **Import Rules**, then browse to the file you want to import and select **Upload.**

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.

Import variables

Import a file of variables and change their type. If there are conflicts, the system renames a new variable automatically.

Before you begin
Ensure a variable file is set up.

Task

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 rules in a policy so that you can then import them to anotherMcAfee ESM.

Task

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, select the **Filter** tab.

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

Filter existing rules to view only those that meet your criteria. By default, rules of a specific type appear in the **Policy Editor** in alphabetical order. You can list them by time or use tags to filter the rules.

Task

1 In the **Rule Types** pane of the **Policy Editor**, select the type of rule you want to filter.

2 Select the **Filter** tab in the **Filters/Tagging** pane.

3 Do any of the following:

- Filter with multiple tags by selecting categories or tags, then click the **Run Query** icon.
- Select more than one category or tag, then click the **or** icon, then click the **Run Query** icon.

  You cannot use the **or** icon to filter fields affected by inheritance (**Action**, **Severity**, **Blacklist**, **Aggregation**, and **Copy Packet**).

- Type the tag's name in the **Type here to search for a tag** field, then select the one you need from the list of options.
- List the rules by the time they were created by clicking the **Sort on Time** icon on the toolbar, then click the **Run Query** icon.
- List the rules in alphabetical order by clicking the **Sort on Name** icon on the toolbar, then click the **Run Query** icon.
- Deselect the filtering by clicking the orange filter icon on the rules display pane title bar.
- Deselect the filter tags by clicking the **Clear All** icon on the toolbar. The tags are deselected but the list of rules remains filtered.
- Filter by signature ID by clicking the **Advanced** bar at the bottom of the **Filter** pane. Then, type the signature ID, then click the **Run Query** icon.
- Filter by name or description. In the **Advanced** pane, enter the name or description. For the results, regardless of case, click the case-insensitive icon Aa.
- Filter by device type, normalized ID, or action. In the **Advanced** pane, click the **Filter** icon. On the **Filter Variables** page, select the variable.
- Compare the differences in the policy-based settings for a rule type and its immediate primary. In the **Advanced** pane, select **View Exceptions**, then click the **Run Query** icon.
- Filter by severity, blacklist, aggregation, copy packet, origin, and rule status by selecting the filter from the drop-down list in each of these fields.
- View only custom rules by selecting **user-defined** in the **Origin** field in the **Advanced** pane, then click the **Run Query** icon.
- View rules created in a specific time period by clicking 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 rule signatures

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

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**.

4 To view the summary of a signature, click the links in the **Signatures** section of the screen.

Retrieve rule updates

McAfee 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.

Before you begin

Set up overrides for the actions taken when the retrieves rules from the server.

Task

1. On the **Policy Editor**, click .
2. On the **Rules Update** line, click **Update**.
3. Set McAfee ESM to retrieve updates automatically or check for updates now.
4. If updates were downloaded manually, click 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, select **Updated**, **New**, or **Update/New** to indicate the type of updated rules you want to view.
   c. Click to run the query.

Clear updated rule status

When you change or add rules to the system, you can deselect these markings once you have had the opportunity to review the updates.

Task

1. In the **Rule Types** pane of the **Policy Editor**, select the type of rule you want to deselect.
2. Do one of the following:
   - Deselect all rule status markings by clicking **Operations**, then select **Clear Updated Rule Status**. Click **All**.
   - To deselect selected rules, click the **Advanced** bar in the **Filters/Tagging** pane. In the **Rule Status** field, select **Updated**, **New**, or **Updated/New** to indicate the type of marking you want to deselect. Click the **Run Query** icon . Select the rules to be deselected, then click **Operation** | **Clear Updated Rule Status** | **Selected**.

Compare rule files

Comparing rule files (applied, current, rollback, or staged) for devices (such as receivers, McAfee Application Data Monitor (ADM), and McAfee Database Event Monitor (DEM) helps you see changes if your current policies to devices.

Task

1. On the system navigation tree, select a device (such as a receiver, ADM, or DEM).
2. Click the **Policy Editor** icon in the actions toolbar, then click **Tools** | **Compare Rule Files**.

If both resulting files are less than about 15.5 MB, they appear in the **Compare Rules Files** table. If either of the files is larger, the system prompts you to download both files.

3 On the **Compare Rules Files** page, make the selections, then click **Compare**.
   - Select the policy states that you want to compare.
     - Applied — Shows the policy that was rolled out to the device.
     - Current — Shows what is real time, but is not rolled out to the device.
     - Rollback — Shows what the policy would be if you were to roll it back to the previous working policy.
     - Staged — Shows the policy that will be applied in the future.
   - View the results of the comparison. Differences between the files are color coded as follows:
     - Blue — Same line exists in both files but the settings have been changed.
     - Red — A line exists in the left file but does not exist in the right file.
     - Green — A line exists in the right file but not the left.

View rule change history

You can view recent rule changes, including summaries of the rules and dates when changes occurred.

Task

1 On the **Policy Editor**, click **Tools** | **Rule Change History**.

2 On the **Rule History** page, view all changes made to rules, or click the **Rule Version** tab to see the newest time stamp for each device that rules are categorized under on the system. This view helps you locate the version of each rule for management and compliance regulations. By default, the system sorts device types alphabetically by name. To sort them by time stamp, click the **Version** column header.

3 Click **Close**.

Assign tags to rules or assets

Assign tags to rules so that you can filter the rules by their tags. McAfee ESM includes predefined tags but you can also create tags unique for your organization.

Variable, preprocessor, or normalization rule types cannot use tags.

Task

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 add tag categories, click the **New Category Tag** icon and naming the category. The system creates a base tag for the new category.
   - To add tags to a category, select it, then click the **New Tag** icon and name the tag.

     To use this tag in event severity calculations, select **Use tag for event severity calculation**, then click **OK**.
   - To change a category or tag, select it, then click the **Edit Tag** icon.
   - To delete a custom tag, select it, then click the **Remove Tag** icon.

Define override actions for downloaded rules

Rules can complete a default action when you download them from the McAfee server. You can define an override action for the rule's default settings. If you do not define an override action, the rules take their default action.

Task

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**.

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.
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 sum of the settings must equal 100. When you change one setting, some or all other settings are affected.

Severity types

Severity type	Descriptions
Asset	An asset is an IP address, optionally in a zone. The system determines an event's asset severity as follows: 1 The system compares the event's destination IP address and destination zone against all assets. If it finds a match, the system uses this asset severity for this event. 2 If the system finds no destination IP address and destination zone match, the system compares the event's source IP address and source zone against all assets. If it finds a match, the system uses the asset severity for this event. 3 If the system finds no matches, the asset severity is 0.
Tag	The system calculates tag severity 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 0. To calculate the tag severity, the system multiplies the number of matching rule and asset tags by 10. The tag severity is limited to 100.

Severity type	Descriptions
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, the system uses the highest severity of all matching asset and rule VA SVEs for the vulnerability severity. Otherwise, the system uses 0.

Define severity weights

Define the severity weights that the system uses to calculate severities for assets, tags, rules, and vulnerability.

Task

1 On the **Policy Editor**, click the **Severity Weights** icon .

2 Define the settings, then click **OK**.

- Drag and drop the markers. The **Assets**, **Tags**, **Rules**, and **Vulnerability** fields reflect these settings.
- For **VA vendor-provided severity** or **VA vendor-provided PCI severity**, select how the system calculates vulnerability severity on incoming data. If you select both, the system uses the greater of the two values when calculating the severity value.

View policy change history

View or export a log of the changes that were made to the policy. This log can hold a maximum of 1 GB of data. When it reaches this limit, the system deletes the oldest files, as needed.

Task

1 On the **Policy Editor**, click the **View Policy Change History** icon .

2 View or export a log, then click **Close**.

Roll out policy changes

Roll out policy changes to one or more devices. Changes you apply at the default policy level are applied to all policies when you roll out changes to devices.

Task

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 policy status indicates a successful rollout. If the rollout command is unsuccessful, a page lists failed commands.

Enable Copy Packet for rules

When you enable **Copy Packet** for a rule, the system copies the packet data McAfee ESM. If enabled, packet data is included in the source event data of an **Internal Event Match** or **Field Match** alarm.

Task

1. On the console, click the **Policy Editor** icon .
2. In the **Rule Types** pane, click the rule type 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**.

12 Using McAfee ESM reports

How reports work

Reports show data from events and flows managed on the McAfee 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® Application Data Monitor
- McAfee® Database Activity Monitoring (McAfee DAM)
- McAfee® Database Event Monitor
- McAfee® Event Reporter

They generate data based on events.

User-defined reports

When creating reports, design the layout by selecting the orientation, size, font, margins, and header and footer. You can also include components, setting them up to display relevant data.

The system saves all layouts, which can be used for multiple reports. When adding reports, you can design new layouts, use existing ones as is, or use existing reports as templates for new reports. You can also remove report layouts.

Add reports

Define which reports you want to run manually or automatically at regular intervals. Select existing report layouts or create reports unique for your organization.

Task

1 From the dashboard, click ☰ and select **Reports**.

2 Define new or existing report settings, then click **Save**.

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	Select the report format: PDF or HTML. • To include views in reports, select **View PDF**. • To generate CSV files from the query results, select **Query CSV.**
Email sent to users or groups	Identify who you want to receive the report. You can send reports or CSV files as email attachments or include them in the email.
File saved to the ESM	Select if you want the report saved in a file. **Prefix** shows the default prefix for the name of the file, which you can change. Once the file has been generated, click **Files** on the **Reports** page to view the report.
File saved to remote location	Save reports to remote locations you identify. To add remote locations, click **manage locations...**.
Choose an existing layout or create a new one	If you selected PDF or HTML format, select an existing layout or create a new one. You can also manage the layouts. • Use folders to organize report layouts. • Import layouts from other locations. If imported layouts include existing images, the system identifies conflicts and suggests the following options: • Keep the image locally but delete it from the report layout. • Replace the image with the image in the report layout. Any layouts that currently use the image that you delete now uses the image imported in the layout. • Rename the image in the report layout automatically and import the layout and image with the new name. • Export layouts. • Summarize the global and individual component filters defined for this report. Filters used appear at the bottom of the report, which identifies the limits defined for the report's data.
Choose a view	For PDF formats, select the view you want to include in the report from the drop-down list.
Choose a predefined query	For CSV formats, select the predefined query.
Enter values to filter	Select which filters to apply to the report components. You can use `contains` and `regex` filters in these fields.

Add report layouts

Design the layout for a report if the predefined layouts do not meet your needs.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. Click **Reports**.
3. Click **Add** to open the **Add Report** page, then complete sections 1, 2, and 3.
4. In section 4, select **Report PDF** or **Report HTML**.
5. In section 5, click **Add** to open the **Report Layout** editor.
6. 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.

Add image components to reports

Select an image to add to the body of a report as a component.

> **Before you begin**
> Verify image files are accessible.

Task

1. From the McAfee ESM dashboard, click ☰ and select **System Properties**.
2. Click **Reports** | **Add** and complete sections 1–4.
3. In section 5, design a new report layout or edit an existing layout.
4. Drag and drop the **Image** icon  on the body section of the layout.
5. Upload a new image or select an existing image.
6. Click **OK** to add the image to the report layout.

Include images in PDFs and reports

Set up McAfee ESM so that 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

1. From the McAfee ESM dashboard, click ☰ and select **System Properties**. Then click **Custom Settings**.
2. Select **Include image in exported PDF from Views or printed reports**.
3. Click **OK**.

Add report conditions

Add conditions so they are available when setting up a report.

Task

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.

Display host names in a report

You can configure reports to use DNS resolution for source and destination IP addresses on reports.

Task

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**).

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

1. From the McAfee ESM dashboard, click ☰ and 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.

View device summary reports

View device summary reports to see the types and number of devices on McAfee ESM, and when each device received events. You can export the reports in comma-separated value (CSV) format.

Task

1. From the McAfee ESM dashboard, click ☰ and select **Configuration**.
2. On the system navigation tree, select McAfee ESM, then click the **Properties** icon .
3. Select **System Information** then click **View Reports**.
4. To view or export a list of devices, select the **Device Type Count** tab.or **Event Time** report.
5. To compare the time of day on the device clocks, select the **Event Time** tab.

Device health status reports

White (informational), yellow (inactivity or device status), or red (critical) health status flags appear next to system, group, or device nodes on the system navigation tree when a health status report is available. When you click the flag, the **Device Status Alerts** page provides you with options to view the information and resolve any issues.

A flag on this type of node...	Opens...
System or group	The **Device Status Alerts Summary** page, which is a summary of the status alerts for the devices associated with the system or group. It can display these status alerts: • **Drive Space** — A hard drive is full or running low on space. Could include the hard drive on the McAfee ESM, redundant McAfee ESM, or remote mount point. • **Critical** — The device is not working properly. • **Warning** — Something on the device is not functioning properly. • **Informational** — The device is working properly but the device status level changed. • **Out of Sync** — The virtual device, data source, or database server settings on the McAfee ESM are out of sync with what is actually on the device. • **Rolled over** — The log table for this device ran out of space so it has rolled over. This means that the new logs are writing over the old logs. • **Inactive** — The device has not generated events or flows in the inactivity threshold time period. • **Unknown** — McAfee ESM could not connect to the device. **Drive space**, **Rolled over**, and **Informational** flags can be resolved by checking the boxes next to the flags and clicking **Clear Selected** or **Clear All**.
Device	The **Device Status Alerts** page, which has buttons that take you to locations for resolving the problem. It might include these buttons: • **Log** — The **System Log** (for Local McAfee ESM) or **Device Log** page shows a summary of all actions that have taken place on the system or device. • **Virtual Devices**, **Data Sources**, **VA Sources**, or **Database Servers** — Lists the devices of this type on the system, allowing you to check for problems. • **Inactive** — The **Inactivity Threshold** page shows the threshold setting for all devices. This flag indicates that the device has not generated an event in the interval specified.

An informational flag appears whenever a subsystem recovers from a warning or critical status. Here is a description of each type of informational flag.

Status	Description and instructions
Bypass mode	The Network Interface Controller (NIC) is in bypass mode. Possible reasons include the failure of a critical system process, manually setting the device in bypass mode, or other failure. To take the device out of bypass mode, go to device **Properties** | **Configuration** | **Interfaces**.
Deep Packet Inspector not running	The Deep Packet Inspector (DPI) has malfunctioned. It might recover without intervention. If not, restart the device.
Firewall alert program (ngulogd) not running	The Firewall Alert Aggregator (FAA) has malfunctioned. It might recover without intervention. If not, restart the device.
Database not running	The McAfee ESM Extreme Database (EDB) server has malfunctioned. Restarting the device might solve the problem, but the database might need to rebuild.

Status	Description and instructions
Control channel not running	The process that services the communication channel with McAfee ESM has failed. A device reboot might remedy the problem.
RDEP or Syslog programs not running	If there is a malfunction with the subsystem that handles the third-party data sources (such as syslog or SNMP), a critical alert is raised. A warning-level alert is raised if the collector hasn't received data from the third-party data source in a certain amount of time. This indicates the data source might be down or not sending data to the Receiver as expected.
System logger not running	The system logger is not responding. A reboot of the device might remedy the problem.
Hard drive partition free space low	The amount of free disk space is critically low.
Fan speed alert	Fans are spinning very slowly or not at all. Until the fan can be replaced, keep the device in an air conditioned room to prevent damage.
Temperature Alert	Temperature of critical components is above a certain threshold. Keep the device in an air conditioned room to prevent permanent damage. Check to see if anything is blocking the airflow through the device.
Network errors	There are network errors or excessive collisions on the network. The cause might be a large collision domain or bad network cables.
Problem with a remote mount point	There is a problem with a remote mount point.
Remote mount point free disk space low	The remote mount point free disk space is low.
All data source collectors that have not received communication from a data source for at least 10 minutes	The Receiver has not received any communication from a data source for at least 10 minutes.
Data source collector not running	There is a malfunction with the subsystem that handles the specific third-party data sources (such as syslog or SNMP). The collector hasn't received any data from the third-party data source in a certain amount of time. The data source may be down or not sending data to the Receiver as expected.
Health Monitor unable to get a valid status from a subsystem	The health monitor was unable to get a valid status from a subsystem.
Subsystem recovery from a warning or critical status	When the health monitor is started and stopped, an informational alert is generated. If the health monitor has trouble communicating with other subsystems on the devices, an alert is also generated. Viewing the event log may provide details on the causes of the warning and critical alerts.

McAfee™
Together is power.