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

**Preface**
- About this guide .................................. 9
- Audience .................................. 9
- Conventions ................................. 9
- Find product documentation ..................... 10

**1 Introduction**
- How McAfee Enterprise Security Manager works .................................. 11
- Devices and what they do .............................. 12

**2 Getting started**
- About FIPS mode .................................. 13
- FIPS mode information ............................ 14
- Select FIPS mode .................................. 14
- Check FIPS integrity ............................. 15
- Adding a keyed device in FIPS mode ....................... 15
- Troubleshooting FIPS mode .......................... 18
- Common Criteria evaluated configuration ..................... 18
- Log on and off ................................... 19
- Customize the logon page .............................. 20
- Update the ESM software .............................. 21
- Obtain and add rule update credentials ......................... 21
- Check for rule updates ............................... 22
- Change language for event logs ............................ 22
- Connecting devices ................................. 23
  - Add devices to the ESM console ......................... 23
  - Select a display type ............................. 24
  - Manage custom display types .......................... 24
  - Manage a group in a custom display type ..................... 24
  - Delete a group or device ............................ 25
  - Delete duplicate devices on the system navigation tree ............... 25
- Console preferences ................................ 26
  - The ESM console .................................. 26
  - Work with console color theme ......................... 26
  - Select console view settings .......................... 27
  - Set console timeout value ........................... 27
  - Select user settings .............................. 27
  - Set up user credentials for McAfee ePO ...................... 28

**3 Configuring the ESM**
- Managing devices .................................. 30
  - View device statistics ............................. 31
  - Add devices to the ESM console ......................... 31
  - About device keys ................................ 32
  - Update the software on a device .......................... 34
Organizing your devices ............................................. 34
Manage multiple devices ............................................. 49
Manage URL links for all devices ................................. 49
View device summary reports ....................................... 49
View a system or device log ......................................... 50
Device health status reports ........................................ 50
Delete a group or device ............................................. 53
Refresh the devices ..................................................... 53
Configuring devices ..................................................... 53
Devices and what they do ............................................ 54
Event Receiver settings .............................................. 55
Enterprise Log Manager (ELM) settings ......................... 103
Advanced Correlation Engine (ACE) settings ................... 117
Application Data Monitor (ADM) settings ....................... 120
Database Event Monitor (DEM) settings ......................... 134
Distributed ESM (DES M) settings ................................ 141
ePolicy Orchestrator settings ...................................... 141
Nitro Intrusion Prevention System (Nitro IPS) settings .......... 147
McAfee Vulnerability Manager settings ........................ 151
McAfee Network Security Manager settings .................... 152
Configuring ancillary services ..................................... 153
General system information ......................................... 153
Configure Remedy server settings ............................... 153
Defining message settings ......................................... 154
Set up NTP on a device .............................................. 155
Configure network settings ........................................ 155
System time synchronization ...................................... 161
Install a new certificate ............................................... 162
Configure profiles ...................................................... 162
SNMP configuration ................................................... 162
Managing the database ............................................... 168
Set up ESM data storage ............................................ 169
Set up ESM VM data storage ..................................... 169
Increase number of available accumulator indexes ............ 169
Set up inactive partitions archive ................................. 170
Set up data retention limits ....................................... 170
Define data allocation limits ...................................... 171
Manage database index settings .................................. 171
Manage accumulator indexing ..................................... 171
View database memory utilization ............................... 172
Working with users and groups ................................... 172
Add a user ................................................................ 173
Select user settings .................................................... 173
Setting up security ..................................................... 173
Set up user credentials for McAfee ePO ......................... 176
Disable or re-enable a user ......................................... 176
Authenticate users to an LDAP server ......................... 177
Set up user groups .................................................... 177
Add a group with limited access .................................. 177
Backing up and restoring system settings ....................... 178
Back up ESM settings and system data ......................... 178
Restore ESM settings ............................................... 179
Restore backed up configuration files .......................... 179
Work with backup files on ESM ................................. 179
Manage file maintenance .......................................... 180
Redundant ESM ....................................................... 180
Contents

Managing the ESM ............................................. 181
  Manage logs ........................................... 183
  Mask IP addresses ...................................... 184
  Set up ESM logging ..................................... 184
  Change language for event logs ......................... 184
  Export and restore communication keys .................... 185
  Regenerate SSH key ................................... 185
  Queries task manager .................................. 185
  Manage queries running on ESM ......................... 186
  Update primary or redundant ESM ....................... 186
  Access a remote device ................................ 187
  Use Linux commands .................................... 187
  Available Linux commands .............................. 187
Using a global blacklist ..................................... 188
  Set up a global blacklist ................................ 189
What is data enrichment .................................. 189
  Add data enrichment sources ........................... 190
  Set up McAfee Real Time for McAfee ePO data enrichment .... 190
  Add Hadoop HBase data enrichment source ............... 190
  Add Hadoop Pig data enrichment source .................. 191
  Add Active Directory data enrichment for user names ....... 192

4 Managing cyber threats ..................................... 193
  Set up cyber threat management ........................ 193
  View cyber threat feed results ........................... 194

5 Working with content packs .............................. 197
Import content packs ....................................... 197

6 Working with alarms ....................................... 199
  How ESM alarms work .................................. 199
  Create an alarm ........................................ 200
    UCAPL alarms ........................................ 201
    Set up correlation alarm to include source events ..... 203
    Add a Field Match alarm ............................... 203
    Add an alarm to rules ................................ 204
    Create an SNMP trap as an action in an alarm ......... 204
    Add a power failure notification alarm ................ 205
    Add a health monitor event alarm ..................... 206
    Copy an alarm ....................................... 213
  Enable or disable alarm monitoring ..................... 213
  Customize summary for triggered alarms and cases .......... 214
  Manage alarm message templates ........................ 214
  Manage alarm audio files ................................ 215
  Manage alarm recipients ................................ 215
  Manage alarms ......................................... 215
    View alarm reports queue ............................. 216
    Manage alarm report files ............................ 216

7 Working with events ....................................... 219
  Events, flows, and logs ................................ 219
    Set up events, flows, and logs downloads ............... 220
    Limit time for data collection ........................ 220
    Define inactivity threshold settings ................... 220
    Get events and flows .................................. 221
    Check for events, flows, and logs ..................... 221
10 Managing policies and rules

Understanding the Policy Editor ................................................. 283

The Policy Tree ........................................................................... 284

Manage policies on the Policy Tree ........................................... 285

Rule types and their properties .................................................. 286

Variables ................................................................................. 287

Preprocessor rules ...................................................................... 289

Firewall rules ............................................................................. 291

Deep packet inspection rules .................................................... 292

Internal rules .............................................................................. 293

Filter rules ................................................................................. 294

ASP rules .................................................................................. 294

Data source rules ....................................................................... 296

Windows events rules ............................................................... 297

ADM rules ................................................................................ 297

DEM rules ................................................................................ 299

Correlation rules ....................................................................... 304

View correlation rule details .................................................... 305

Add custom ADM, database, or correlation rules .................. 305

ESM rules ................................................................................ 312

Normalization ......................................................................... 312

Enable Copy Packet .................................................................. 312

Default Policy settings .............................................................. 313

Alerts Only Mode ..................................................................... 313

Set up Oversubscription Mode ................................................ 313

View policy update status for devices ..................................... 314

Rule operations ......................................................................... 314

Manage rules ............................................................................ 314

Import rules .............................................................................. 315

Import variables ....................................................................... 316

Export rules .............................................................................. 316

Set rules to auto-blacklist ......................................................... 317

Filter existing rules .................................................................. 317

View a rule’s signature ............................................................. 318

Retrieve rule updates ............................................................... 319

Clear updated rule status ......................................................... 319

Compare rule files ..................................................................... 320

View the rule change history .................................................... 320

Create a new watchlist of rules ............................................... 321

Add rules to a watchlist ............................................................ 321

Assign tags to rules or assets ................................................... 322

Modify aggregation settings ..................................................... 322

Override action on downloaded rules .................................... 323

Severity weights ....................................................................... 323
Preface

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

Contents

» About this guide
» Find product documentation

About this guide

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

Audience

McAfee documentation is carefully researched and written for the target audience. The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company’s security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**
  Title of a book, chapter, or topic; a new term; emphasis.
- **Bold**
  Text that is strongly emphasized.
- **User input, code, message**
  Commands and other text that the user types; a code sample; a displayed message.
- **Interface text**
  Words from the product interface like options, menus, buttons, and dialog boxes.
- **Hypertext blue**
  A link to a topic or to an external website.
- **Note**: Additional information, like an alternate method of accessing an option.
Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

**Task**


2. In the Knowledge Base pane, click a content source:
   - Product Documentation to find user documentation
   - Technical Articles to find KnowledgeBase articles

3. Select Do not clear my filters.

4. Enter a product, select a version, then click Search to display a list of documents.
Introduction

McAfee Enterprise Security Manager (McAfee ESM) allows security and compliance professionals to collect, store, analyze, and act upon risks and threats from a single location.

Contents

- How McAfee Enterprise Security Manager works
- Devices and what they do

How McAfee Enterprise Security Manager works

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

ESM is composed of three layers:

- **Interface** – A browser program that provides the user’s interface to the system (referred to as the ESM console).

- **Data storage, management, and analysis** – Devices that provide all necessary data manipulation services, including configuration, reporting, visualization, and searching. ESM (required), Advanced Correlation Engine (ACE), Distributed ESM (DESM), and Enterprise Log Manager (ELM) perform these functions.

- **Data acquisition** – Devices that provide the interfaces and services that acquire data from the user’s network environment. Nitro Intrusion Prevention System (IPS), Event Receiver (Receiver), Application Data Monitor (ADM), and Database Event Monitor (DEM) perform these functions.
All command, control, and communication functions between the components are coordinated through secure communication channels.

**Devices and what they do**

The ESM enables you to administer, manage, and interact with all physical and virtual devices in your security environment.

**See also**

*Event Receiver settings* on page 55
*Enterprise Log Manager (ELM) settings* on page 103
*Application Data Monitor (ADM) settings* on page 120
*Database Event Monitor (DEM) settings* on page 134
*Advanced Correlation Engine (ACE) settings* on page 117
*Distributed ESM (DESM) settings* on page 141
*ePolicy Orchestrator settings* on page 141
*Nitro Intrusion Prevention System (Nitro IPS) settings* on page 147
Getting started

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

Contents
- About FIPS mode
- Common Criteria evaluated configuration
- Log on and off
- Customize the logon page
- Update the ESM software
- Obtain and add rule update credentials
- Check for rule updates
- Change language for event logs
- Connecting devices
- Console preferences

About FIPS mode

The Federal Information Processing Standard (FIPS) consists of publicly announced standards developed by the United States Federal government. If you are required to meet these standards, you must operate this system in FIPS mode.

See also
FIPS mode information on page 14

Contents
- FIPS mode information
- Select FIPS mode
- Check FIPS integrity
- Adding a keyed device in FIPS mode
- Troubleshooting FIPS mode
FIPS mode information
Due to FIPS regulations, some ESM features aren't available, some available features are not compliant, and some features are only available when in FIPS mode. These features are noted throughout the document and are listed here.

<table>
<thead>
<tr>
<th>Feature status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removed features</td>
<td>• High Availability Receivers.</td>
</tr>
<tr>
<td></td>
<td>• GUI Terminal.</td>
</tr>
<tr>
<td></td>
<td>• Ability to communicate with the device using SSH protocol.</td>
</tr>
<tr>
<td></td>
<td>• On the device console, the root shell is replaced by a device management menu.</td>
</tr>
<tr>
<td>Features available only in FIPS mode</td>
<td>• There are four user roles that do not overlap: <strong>User</strong>, <strong>Power User</strong>, <strong>Audit Admin</strong>, and <strong>Key &amp; Certificate Admin</strong>.</td>
</tr>
<tr>
<td></td>
<td>• All <strong>Properties</strong> pages have a <strong>Self-Test</strong> option that allows you to verify that the system is operating successfully in FIPS mode.</td>
</tr>
<tr>
<td></td>
<td>• If FIPS failure occurs, a status flag is added to the system navigation tree to reflect this failure.</td>
</tr>
<tr>
<td></td>
<td>• All <strong>Properties</strong> pages have a <strong>View</strong> option that, when clicked, opens the <strong>FIPS Identity Token</strong> page. It displays a value that must be compared to the value shown in those sections of the document to ensure that FIPS hasn't been compromised.</td>
</tr>
<tr>
<td></td>
<td>• On <strong>System Properties</strong></td>
</tr>
<tr>
<td></td>
<td>• When you click <strong>Import Key</strong> or <strong>Export Key</strong> on <strong>IP Properties</strong></td>
</tr>
<tr>
<td></td>
<td>• On the <strong>Add Device Wizard</strong>, TCP protocol is always set to Port 22. The SSH port can be changed.</td>
</tr>
</tbody>
</table>

Select FIPS mode
The first time you log on to the system you are prompted to select whether you want the system to operate in FIPS mode. Once this selection is made, it can't be changed.

Task
For option definitions, click ? in the interface.

1  The first time you log on to the ESM:
   a  In the **Username** field, type **NGCP**.
   b  In the **Password** field, type **security.4u**.

   You are prompted to change your password.

2  Enter and confirm your new password.

3  On the **Enable FIPS** page, click **Yes**.

   The **Enable FIPS** warning displays information requesting confirmation that you want this system to operate in FIPS mode permanently.

4  Click **Yes** to confirm your selection.
Check FIPS integrity

If you are operating in FIPS mode, FIPS 140-2 requires software integrity testing on a regular basis. This testing must be performed on the system and each device.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, and make sure that **System Information** is selected.

2. Do any of the following.

<table>
<thead>
<tr>
<th>In this field...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FIPS Status</strong></td>
<td>View the results of the most recent FIPS self-test performed on the ESM.</td>
</tr>
<tr>
<td><strong>Test or FIPS Self-Test</strong></td>
<td>Run the FIPS self-tests, which test the integrity of the algorithms used within the crypto-executable. The results can be viewed on the <strong>Message Log</strong>.</td>
</tr>
<tr>
<td></td>
<td>⚠️ If the FIPS self-test fails, FIPS is compromised or device failure is occurring. Contact McAfee Support.</td>
</tr>
<tr>
<td><strong>View or FIPS Identity</strong></td>
<td>Open the <strong>FIPS Identity Token</strong> page to perform power-up software integrity testing. Compare the value below to the public key that appears on this page:</td>
</tr>
<tr>
<td></td>
<td>-----BEGIN PUBLIC KEY-----</td>
</tr>
<tr>
<td></td>
<td>MIICJANBgkqhkiG9w0BAQEFAAOCAg8AMIICgKCAgEA18FWOP2mvVjvTTxkhGqkJDgA+sx0jb+V3y1CkYG0HHzNAdum9yuMn69GNgXm7150cKv2+rz6axBrUCZ3XX1jCGWmsb8YZjoNp/FLuy1Ye7IXi5/NRm2uhjzjdOjgFv105kgxVf/aBj9qZFJ</td>
</tr>
<tr>
<td></td>
<td>KBbHMzYEBwdyscQUc56u3mkaBtp4rydfrM6ytkuOsZgQuPHKHyaaQjlnbV5LfrLa06HQSrzHYHlcF/Yog+QHJ6C5RA1lk8MPyFG9RhDNwcnq3sY8QjQMbI55SDobbK0GPOOucG8vWDWdxSiFbLQdjiVsmB0zwH61OCkGTidayMk12rHd+2BAe17YQBv8EFjal5wv8aQKrWDfimlb9vmC+sk+Rwo/E/uRn3El4+RXouH19Jfi9219qXZejCViYv2XahhuyX0p8sro/0BMtIab3djJgqXMcI9QjEm3j/ZyUpWtNkaHq8Bg5E1e</td>
</tr>
<tr>
<td></td>
<td>da1j0B70/kvef1T/ZOb3O90b5K3tv+35i3K3yapaY/qBm9var6xVNYvGhHzrJv0F0n5fjyddWuXL1U+hMT02YE33T3s4U4j ThomTVSDtJ087hLT5t/hCz6A33Hzh7gk8Q895NsmL/p0RAjJzJ3-mGyoUA1dID2u6sYQ6NxtGcn640a5A2zAOQdx/M8R85+NKjgJ1nlG3vr+/25KscB3KDY3AKYECawEAQ==</td>
</tr>
<tr>
<td></td>
<td>-----END PUBLIC KEY-----</td>
</tr>
<tr>
<td></td>
<td>⚠️ If this value and the public key don't match, FIPS is compromised. Contact McAfee Support.</td>
</tr>
</tbody>
</table>

Adding a keyed device in FIPS mode

There are two methods in FIPS mode to add a device that has already been keyed to an ESM. This terminology and file extensions are useful as you follow these processes.

**Terminology**

- **Device key** — Contains the management rights that an ESM has for a device, and is not used for crypto.

- **Public key** — The ESM public SSH communication key, which is stored in the authorized keys table of a device.
• **Private key** — The ESM private SSH communication key, which is used by the SSH executable on an ESM to establish the SSH connection with a device.

• **Primary ESM** — The ESM that was originally used to register the device.

• **Secondary ESM** — The additional ESM that communicates with the device.

**File extensions for the different export files**

- **.exk** — Contains the device key.
- **.puk** — Contains the public key.
- **.prk** — Contains the private key and the device key.

**Backup and restore information for a device in FIPS mode**

This method is used to back up and restore communication information for a device on the ESM. It is primarily intended for use in the event of a failure that requires ESM replacement. If the communication information is not exported prior to the failure, communication with the device can't be re-established. This method exports and imports the .prk file.

The private key for the primary ESM is used by the secondary ESM to establish communication with the device initially. Once communication is established, the secondary ESM copies its public key to the device's authorized keys table. The secondary ESM then erases the private key for the primary ESM, and initiates communication with its own public or private key pair.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Export the .prk file from the primary ESM | 1 On the system navigation tree of the primary ESM, select the device with communication information you want to back up, then click the **Properties** icon.  
2 Select **Key Management**, then click **Export Key**.  
3 Select **Backup SSH Private key**, then click **Next**.  
4 Type and confirm a password, then set the expiration date.  
   
   After the expiration date passes, the person who imports the key is unable to communicate with the device until another key is exported with a future expiration date. If you select **Never Expire**, the key never expires if imported into another ESM.  
5 Click **OK**, select the location to save the .prk file created by the ESM, then log out of the primary ESM. |
| Add a device to the secondary ESM and import the .prk file | 1 On the system navigation tree of the secondary device, select the system or group level node you want to add the device to.  
2 From the actions toolbar, click **Add Device**.  
3 Select the type of device that you want to add, then click **Next**.  
4 Enter a name for the device that is unique in this group, then click **Next**.  
5 Enter the target IP address of the device, enter the FIPS communication port, then click **Next**.  
6 Click **Import Key**, browse to the previously exported .prk file, then click **Upload**.  
   
   Type the password specified when this key was initially exported.  
7 Log out of the secondary ESM. |
Enable communication with multiple ESM devices in FIPS mode

You can allow multiple ESMs to communicate with the same device by exporting and importing .puk and .exk files.

This method uses two export and import processes. First, the primary ESM is used to import the secondary ESM device exported .puk file and send the contained secondary ESM public key to the device, thus allowing both ESM devices to communicate with the device. Second, the device's .exk file is exported from the primary ESM and imported into the secondary ESM, thus giving the secondary ESM the ability to communicate with the device.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Export the .puk file from the secondary ESM | 1 On the System Properties page of the secondary ESM, select ESM Management.  
2 Click Export SSH, then select the location to save the .puk file.  
3 Click Save, then log out. |
| Import the .puk file to the primary ESM | 1 In the system navigation tree of the primary ESM, select the device you want to configure.  
2 Click the Properties icon, then select Key Management.  
3 Click Manage SSH Keys.  
4 Click Import, select the .puk file, then click Upload.  
5 Click OK, then log out of the primary ESM. |
| Export the device's .exk file from the primary ESM | 1 In the system navigation tree of the primary ESM, select the device you want to configure.  
2 Click the Properties icon, then select Key Management.  
3 Click Export Key, select the backup device key, then click Next.  
4 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 ESM.  
5 Select the .exk file privileges, then click OK.  
6 Select the location to save this file, then log out of the primary ESM. |
| Import the .exk file to the secondary ESM | 1 In the system navigation tree of the secondary device, select the system or group level node that you want to add the device to.  
2 From the actions toolbar, click Add Device.  
3 Select the type of device you want to add, then click Next.  
4 Enter a name for the device that's unique to this group, then click Next.  
5 Click Import Key, then browse to the .exk file.  
6 Click Upload and enter the password that was specified when this key was initially exported.  
7 Log out of the secondary ESM. |
Troubleshooting FIPS mode

Issues might arise when operating the ESM in FIPS mode.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description and resolution</th>
</tr>
</thead>
</table>
| Can't talk to the ESM | • Check the LCD on the front of the device. If it says FIPS Failure, contact McAfee Support.  
  • Check for an error condition through the HTTP interface by viewing the ESM FIPS Self-test webpage in a browser.  
    - If a single digit 0 is displayed, indicating that the device has failed a FIPS self-test, reboot the ESM device and attempt to correct the problem. If the failure condition persists, contact Support for further instructions.  
    - If a single digit 1 is displayed, the communication problem is not due to FIPS failure. Contact Support for further troubleshooting steps. |
| Can't talk to the device | • If there is a status flag next to the device on the system navigation tree, place the cursor over it. If it says FIPS Failure, contact McAfee Support by going to the support portal.  
  • Follow the description under the Can't talk to the ESM issue. |
| The file is invalid error when adding a device | You cannot export a key from a non-FIPS device and then import it to a device operating in FIPS mode. Also, you cannot export a key from an FIPS device and then import it to a non-FIPS device. This error appears when you attempt either scenario. |

Common Criteria evaluated configuration

The McAfee appliance needs to be installed, configured, and operated in a specific way to be in compliance with the Common Criteria evaluated configuration. Keep these requirements in mind when you are setting up your system.

<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Physical | The McAfee appliance must be:  
  • Protected from unauthorized physical modification.  
  • Located within controlled access facilities, which prevent unauthorized physical access. |
| Intended usage | The McAfee appliance must:  
  • Have access to all the network traffic to perform its functions.  
  • Be managed to allow for address changes in the network traffic that the Target of Evaluation (TOE) monitors.  
  • Be scaled to the network traffic that it monitors. |
<table>
<thead>
<tr>
<th>Type</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Personnel  | • There must be one or more competent individuals assigned to manage the McAfee appliance and the security of the information it contains. On-site assistance with installation and configuration and on-site training for the operation of the appliance is provided by McAfee engineers for each McAfee customer.  
• The authorized administrators are not careless, willfully negligent, or hostile, and follow and abide by the instructions provided by the McAfee appliance documentation.  
• The McAfee appliance must only be accessed by authorized users.  
• Those responsible for the McAfee appliance must ensure that all access credentials are protected by users in a manner that is consistent with IT security. |
| Other      | • Do not apply software updates to the McAfee appliance as it will result in a configuration other than the Common Criteria evaluated configuration. Contact McAfee Support to obtain a certified update.  
• On a Nitro IPS device, enabling the **Watchdog Timer** and **Force Bypass** settings in the **Network Interface Settings** page results in a configuration other than the Common Criteria evaluated configuration.  
• On a Nitro IPS device, using an oversubscription mode setting other than drop will result in a configuration other than the Common Criteria evaluated configuration.  
• Enabling the **Login Security** feature with a RADIUS server will result in secure communication. The IT environment provides for secure transmission of data between the TOE and external entities and external sources. External authentication services can be provided by a RADIUS server.  
• Using the **Smart Dashboard** functionality of the Check Point firewall console is not part of the TOE.  
• Using Snort Barnyard is not part of the TOE.  
• Using the MEF Client is not part of the TOE.  
• Using the Remedy Ticket System is not part of the TOE. |

### Log on and off

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

**Task**

For option definitions, click ? in the interface.

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. Click **Login**, select the language for the console, then type the default user name and password.
   - **Default user name:** NGCP
   - **Default password:** security.4u

3. Click **Login**, read the **End User License Agreement**, then click **Accept**.

4. Change your user name and password, then click **OK**.
5 Select whether to enable FIPS mode.

If you are required to work in FIPS mode, you must enable it the first time you log on to the system so that all future operations with McAfee devices are in FIPS mode. We recommend that you do not enable FIPS mode if you are not required to. For more information, see About FIPS mode.

6 Follow the instructions to get your user name and password, which are necessary for access to rule updates.

7 Perform initial ESM configuration:
   a Select the language to be used for system logs.
   b Select the time zone where this ESM is and the date format to be used with this account, then click Next.
   c Define the settings on the Initial ESM Configuration wizard pages. Click the Show Help icon on each page for instructions.

8 Click OK, then click the links for help in getting started or to see the new features that are available in this version of ESM.

9 When you complete your work session, log off using one of these methods:
   • If no pages are open, click logout on the system navigation bar in the top-right corner of the console.
   • If pages are open, close the browser.

See also
About FIPS mode on page 13

---

**Customize the logon page**

You can customize the logon page to add text, such as company security policies, or a logo.

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, select System Properties | Custom Settings.

2 Do any of the following:
## Update the ESM software

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

To update a primary or redundant ESM, see *Update primary or redundant ESM*.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **ESM Management**.
2. On the **Maintenance** tab, click **Update ESM**.
3. Select the file you want to use to update your ESM, then click **OK**.

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

**See also**

*Update primary or redundant ESM* on page 186

## Obtain and add rule update credentials

The 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**

For option definitions, click ? in the interface.

1. Obtain your credentials by sending an email message to Licensing@McAfee.com with this information:
   - McAfee grant number
   - Account name
   - Address
Check for rule updates

The rule signatures used by Nitro IPS to examine network traffic are continuously updated by the McAfee Signature Team and are available for download from the central server at McAfee. These rule updates can be retrieved automatically or manually.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then make sure that System Information is selected.

2. In the Rule Updates field, check that your license hasn’t expired.
   
   If your license has expired, see Obtain and add rule update credentials.

3. If your license is valid, 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.

See also
Obtain and add rule update credentials on page 21

Change language for event logs

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

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties | ESM Management.

2. Click System Locale, select a language from the drop-down list, then click OK.
Connecting devices

Connect both physical and virtual devices to McAfee ESM to enable real-time forensics, application and database monitoring, advanced rule- and risk-based correlation, and compliance reporting. As you increase the number of devices on your system, organize them logically. For example, if you have offices in various locations, display those devices by the zone they are in. You can use the predefined displays, as well as design your own custom displays. To further organize devices, you can group them within each custom display.

Contents

- Add devices to the ESM console
- Select a display type
- Manage custom display types
- Manage a group in a custom display type
- Delete a group or device
- Delete duplicate devices on the system navigation tree

Add devices to the ESM console

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

Before you begin

Set up and install the devices (see McAfee Enterprise Security Manager Installation Guide).

Task

1. On the system navigation tree, click Local ESM or a group.
2. On the actions toolbar, click the Add Device icon.
3. Select the type of device you are adding, then click Next.
4. In the Device Name field, enter a name that is unique in this group, then click Next.
5. Provide the information requested:
   - For McAfee ePO devices — Select a Receiver, type the credentials required to log on to the web interface, then click Next. Type the settings to use for communicating with the database.
     
     Select Require user authentication to limit access to those users who have the username and password for the device.
   
   - For all other devices — Type the target IP address or URL for the device, then type a target SSH port number that is valid to be used with the IP address.
6. Select whether or not to use Network Time Protocol (NTP) settings on the device, then click Next.
7. If you have a key that you want to import, select Import Key (not available on ELM or Receiver/Log Manager Combo device); otherwise, click Key Device.

Device keys that were originally exported from a pre-8.3.x ESM have no knowledge of the 8.4.0 communication model. Upon upgrade you were required to re-key the device. To have access to devices in versions 9.0.0 or later, you must re-export the key for this device from an ESM that is 8.5.0 or later. Be sure to set any privileges required for the device, like the Configure Virtual Devices privilege.

8. Enter a password for this device, then click Next.

The ESM tests device communication and reports on the status of the connection.
Select a display type
Select the way you want to display the devices in the system navigation tree.

Before you begin
To select a custom display, you must add it to the system first (see Manage 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 organization of the devices on the navigation tree changes to reflect the type you selected for the current work session.

Manage custom display types
You can define how you want the devices on the system navigation tree to be organized by adding, editing, or deleting custom display types.

Task
For option definitions, click ? in the interface.
1 On the system navigation pane, click the display type drop-down arrow.
2 Do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Add a custom display type | 1 Click Add Display.  
                          | 2 Fill in the fields, then click OK. |
| Edit a custom display type | 1 Click the Edit icon next to the display type you want to edit.  
                          | 2 Make changes to the settings, then click OK. |
| Delete a custom display type | Click the Delete icon next to the display type you want to delete. |

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

Before you begin
Add a custom display type (see Manage custom display types).

Task
For option definitions, click ? in the interface.
1 On the system navigation pane, click the display type drop-down list.
2 Select the custom display, then do one of the following:
### To... | Do this...
---|---
Add a new group | 1 Click a system or group node, then click the **Add Group** icon on the actions toolbar.
| | 2 Fill in the fields, then click **OK**.
| | 3 Drag-and-drop devices on the display to add them to the group.
| | If the device is part of a tree on the display, a duplicate device node is created. You can then delete the duplicate on the system tree.
Edit a group | Select the group, click the **Properties** icon, then make changes on the **Group Properties** page.
Delete a group | Select the group, then click the **Delete Group** icon. The group and the devices that are in it are deleted from the custom display. The devices are not deleted from the system.

**See also**
*Manage custom display types on page 24*

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

**Task**
For option definitions, click ? in the interface.

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

2 When prompted to confirm, click **OK**.

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

**Task**
For option definitions, click ? in the interface.

1 On the system navigation pane, click the display type drop-down list.

2 Select the **Edit** icon next to the display that includes the duplicate devices.

3 Deselect the duplicate devices, then click **OK**.

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

You can customize several features on the ESM console by changing the color theme, date and time format, timeout value, and several default settings. You can also set up McAfee ePolicy Orchestrator (McAfee ePO) credentials.

The ESM console

The ESM console gives you real-time visibility to activity on your devices, as well as quick access to alarm notifications and assigned cases.

1. System navigation toolbar for general setup functions.
2. Icons to access pages that are used frequently.
3. Actions toolbar to select functions necessary to configure each device.
4. System navigation pane to view the devices on the system.
5. Alarms and Cases pane to view alarm notifications and assigned open cases.
6. Views pane for event, flow, and log data.
7. View toolbar to create, edit, and manage views.
8. Filters pane to apply filtering to event-based or flow-based views of data.

Work with console color theme

Customize the ESM console by selecting an existing color theme or designing your own. You can also edit or delete custom color themes.
Task
For option definitions, click ? in the interface.

1. On the system navigation bar of the ESM console, click options.
2. Select an existing color theme, or add, edit, or remove a custom theme.
3. If you click Add or Edit, select the colors for the custom theme, then click OK.
   If you added a new theme, a thumbnail of your colors is added to the Select a theme section.
4. Click OK to save your settings.

Select console view settings
Set the default settings for the views on the ESM console.
On this page, you can set the system to do this:
• Update the data automatically on an open view
• Change the views that open by default when you start the system
• Change the views that open when you select Summarize on an event or flow view

Task
For option definitions, click ? in the interface.

1. On the system navigation bar of the ESM console, click options.
2. On the Views page, select your preferences, then click OK.

Set console timeout value
The current session on the ESM console remains open as long as there is activity. Define how long there can be no activity before the session closes.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties | Login Security.
2. In UI Timeout Value, select the number of minutes that must pass with no activity, then click OK.
   If you select zero (0), the console stays open indefinitely.

Select user settings
The User Settings page gives you the option to change several default settings. You can change the time zone, date format, password, default display, and console language. You can also choose whether to show disabled data sources, the Alarms tab, and the Cases tab.

Task
For option definitions, click ? in the interface.

1. On the system navigation bar of the ESM console, click options.
2. Verify that User Settings is selected.
3. Make changes to the settings as needed, then click OK.
The console changes its appearance based on your settings.

**Set up user credentials for McAfee ePO**

You can limit access to a McAfee ePO device by setting up user credentials.

**Before you begin**

The McAfee ePO device must not be set up to require global user authentication (see Set up global user authentication).

**Task**

For option definitions, click ? in the interface.

1. On the system navigation bar of the ESM console, click options, then select ePO Credentials.
2. Click the device, then click Edit.

   If the status column for the device says Not Required, the device is set up for global user authentication. You can change the status on the Connection page for the device (see Change connection with ESM).

3. Type the user name and password, test the connection, then click OK.

To access this device, users need the user name and password you added.
Configuring the ESM

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

Contents

- Managing devices
- Configuring devices
- Configuring ancillary services
- Managing the database
- Working with users and groups
- Backing up and restoring system settings
- Managing the ESM
- Using a global blacklist
- What is data enrichment
Managing devices

The system navigation pane lists the devices added to the system. You can perform functions on one or more devices and organize them as needed. You can also view health status reports when systems are flagged to resolve existing issues.

Table 3-1 Feature definitions

<table>
<thead>
<tr>
<th>This feature...</th>
<th>Allows you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Actions toolbar</td>
<td>Select an action to be performed on devices in the system navigation tree.</td>
</tr>
<tr>
<td>Properties icon</td>
<td>Configure settings for the system or device selected in the system navigation tree.</td>
</tr>
<tr>
<td>Add devices icon</td>
<td>Add devices to the system navigation tree.</td>
</tr>
<tr>
<td>Health status flags</td>
<td>View device status alerts.</td>
</tr>
<tr>
<td>Multi-device management</td>
<td>Start, stop, restart, and update multiple devices individually.</td>
</tr>
<tr>
<td>Get events and flows</td>
<td>Retrieve events and flows for devices you select.</td>
</tr>
<tr>
<td>Delete a device</td>
<td>Delete the selected device.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refresh the data for all devices.</td>
</tr>
</tbody>
</table>
Table 3-1 Feature definitions (continued)

<table>
<thead>
<tr>
<th>This feature...</th>
<th>Allows you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2 Display type</strong></td>
<td>Select the way you want to organize the devices on the tree. The ESM comes with three predefined types:</td>
</tr>
<tr>
<td><strong>Physical Display</strong></td>
<td>Lists devices hierarchically. The first level is system nodes (Physical Display, Local ESM, and Local ESM base device). The second level is individual devices, and all other levels are the sources you add to the devices (data source, virtual device, and others). Base devices are automatically added under the Local ESM, data source, virtual device, and database server nodes. They have a grayed-out icon and are in parentheses.</td>
</tr>
<tr>
<td><strong>Device Type Display</strong></td>
<td>Groups devices by type of device (Nitro IPS, ADM, DEM).</td>
</tr>
<tr>
<td><strong>Zone Display</strong></td>
<td>Organizes devices by zone, which you define using the Zone Management feature.</td>
</tr>
<tr>
<td>You can also add custom display types (see Organizing your devices).</td>
<td></td>
</tr>
<tr>
<td><strong>3 Quick search</strong></td>
<td>Perform a quick search for a device on the system navigation tree.</td>
</tr>
<tr>
<td><strong>4 System navigation tree</strong></td>
<td>View the devices on the system.</td>
</tr>
</tbody>
</table>

See also

- Organizing your devices on page 34
- Device health status reports on page 50
- Manage multiple devices on page 49

View device statistics

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

**Before you begin**
Verify that you have the Device Management permission.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the relevant device, then click the Properties icon).
2. Navigate through the options and tabs until you find View Statistics.
3. Click View Statistics.

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

Add devices to the ESM console

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

**Before you begin**

Set up and install the devices (see McAfee Enterprise Security Manager Installation Guide).
**Task**

1. On the system navigation tree, click Local ESM or a group.

2. On the actions toolbar, click the Add Device icon.

3. Select the type of device you are adding, then click Next.

4. In the **Device Name** field, enter a name that is unique in this group, then click Next.

5. Provide the information requested:
   - For McAfee ePO devices — Select a Receiver, type the credentials required to log on to the web interface, then click Next. Type the settings to use for communicating with the database.
     
     ![Select Require user authentication to limit access to those users who have the username and password for the device.]

   - For all other devices — Type the target IP address or URL for the device, then type a target SSH port number that is valid to be used with the IP address.

6. Select whether or not to use Network Time Protocol (NTP) settings on the device, then click Next.

7. If you have a key that you want to import, select Import Key (not available on ELM or Receiver/Log Manager Combo device); otherwise, click Key Device.

   ![Device keys that were originally exported from a pre-8.3.x ESM have no knowledge of the 8.4.0 communication model. Upon upgrade you were required to re-key the device. To have access to devices in versions 9.0.0 or later, you must re-export the key for this device from an ESM that is 8.5.0 or later. Be sure to set any privileges required for the device, like the Configure Virtual Devices privilege.]

8. Enter a password for this device, then click Next.

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

**About device keys**

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

We recommend that all keys be exported to an alternate, password-encrypted file. They can then be imported to restore communication to a device in the case of an emergency or to export a key to another device.

All settings are stored on the ESM, which means that the ESM console is aware of the keys maintained on the ESM and does not need to import a device key if the ESM is already successfully communicating with the device.

For example, you might make a backup of your settings (which includes device keys) on Monday, then re-key one of your devices on Tuesday. If on Wednesday you realize you needed to restore Monday’s settings, you import the key created Tuesday after the settings restoration was complete. Although the restoration reverts the device key to what it was on Monday, the device is still listening only for traffic encoded with Tuesday’s key. This key has to be imported before communication with the device is possible.

We recommend not importing a device key into a separate ESM. The export key is used to reinstall a device into the managing ESM for the device, for device management right roles. If you import a device into a second ESM, several device features are not usable, including policy management, ELM logging and management, and data source and virtual device settings. Device administrators can
overwrite settings on the device from another ESM. We recommend that you use a single ESM to manage devices attached to it. A DESM can handle the data collection from devices attached to another ESM.

**Key a device**

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.

2. Click Key Management | Key Device.

   If the device has an established connection and can communicate with the ESM, the Key Device Wizard opens.

3. Type a new password for the device, then click Next.

4. Click Export Key, then complete the Export Key page, or click Finish if you're not going to export it at this time.

**Export a key**

After keying a device, export the key to a file.

If your system is operating in FIPS mode, don't follow this procedure. See Adding a keyed device in FIPS mode for the correct process.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.

2. Click Key Management | Export Key.

3. Define the settings on the Export Key page, then click OK.

   The ESM creates the export key file and asks if you want to export it.

4. Click Yes, then select where you want the file saved.

   We recommend that you export a personal backup copy of the device key that is set to Never Expire and includes all privileges.

**Import a key**

Import a key to restore ESM to previous settings or to use it in another ESM or legacy console.

If your device is version 9.0 or later, you can only import a key from an ESM that is version 8.5 or later.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.

2. Click Key Management | Import Key.
3 Locate and select the saved key file.

4 Click Upload, then type the password that was set when this key was exported.

When the key is successfully imported, a page displays the status.

**Manage SSH keys**

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

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, select a device, then click the Properties icon.

2 Click Key Management, then click Manage SSH Keys.

   The Manage SSH Keys page lists the IDs for the ESM that the device communicates with.

3 Highlight the ID and click Delete to stop communication with one of the systems listed.

4 Confirm the deletion, then click OK.

**Update the software on a device**

If the software on your device is out of date, upload a new version of the software from a file on the ESM or your local computer.

**Before you begin**

If you’ve had your system for more than 30 days, you must obtain and install your permanent credentials to access the updates (see Obtain and add rule update credentials).

   If you must comply with Common Criteria and FIPS regulations, do not update the ESM in this way. Call McAfee support to obtain a certified update.

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, select a device, then click the Properties icon.

2 Click device Management | Update Device.

3 Select an update from the table or click Browse to locate it on your local system.

The device restarts with the updated software version.

**Organizing your devices**

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

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

You can use the three predefined displays and you can design custom displays. Within each custom display, you can add groups to further organize the devices.
Set up network traffic control on a device
Define a maximum data output value for Receiver, ACE, ELM, Nitro IPS, ADM, and DEM devices. This feature is helpful when you have bandwidth restrictions and need to control the amount of data that can be sent out by each of these devices. The options are kilobits (Kb), megabits (Mb), and gigabits (Gb) per second.

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

Task
For option definitions, click ? in the interface.

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

2 Click the Configuration option for the device, click Interfaces, then click the Traffic tab.

The table lists the existing controls.

3 To add controls for a device, click Add, enter the network address and mask, set the rate, then click OK.

   If you set the mask to zero (0), all data sent is controlled.

4 Click Apply.

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

Device configuration
The Configuration page for each device provides options to configure device settings such as network interface, SNMP notifications, NTP settings, and ELM logging.

Set up network interfaces
Interface settings determine how the ESM connects to the device. You must define these for each device.

Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select a device, then click the Properties icon.

2 Click the device's Configuration option, then click Interfaces.

3 Enter the data as requested, then click Apply.

All changes are pushed to the device and take effect immediately. Upon applying changes, the device re-initializes, causing all current sessions to be lost.

Managing network interfaces
Communication with a device can take place using the public and private interfaces of the traffic paths. This means that the device is invisible in the network because it doesn’t require an IP address.

Management interface
Alternately, network administrators can configure a management interface with an IP address for communication between the ESM and the device. These features of a device require the use of a management interface:
• Full control of bypass network cards
• Use of NTP time synchronization
• Device-generated syslog
• SNMP notifications

Devices are equipped with at least one management interface, which gives the device an IP address. With an IP address, the device can be accessed directly by the ESM 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.

For a device running in Nitro IPS mode, there must be two interfaces for each path of network traffic. For IDS mode, there must be a minimum of two network interfaces in the device. You can configure more than one management network interface in the device.

**Bypass NIC**

A device in bypass mode allows all traffic to pass, including malicious traffic. Under normal circumstances, you can have a one- to three-second loss of connection when the device switches to bypass mode, and an 18-second loss when it switches out. Being connected to certain switches, such as some models of Cisco Catalyst, can change these numbers. In this case, you can have a 33-second loss of connection when the device switches to bypass mode and when it switches out.

If you have the scenario where it takes 33 seconds to reestablish communications, you can enable port fast on the switch port and manually set the speed and duplex to get the times back to normal. Be sure to set all four ports (switch, both on Nitro IPS, and other device) to the same setting or you might have a negotiation problem in bypass mode (see Set up bypass NICs).

The available bypass options depend on the type of bypass NIC in the device, Type 2 or Type 3.

**Add static routes**

A static route is a set of instructions about how to reach a host or network that is not available through the default gateway.

**Task**

For option definitions, click ? in the interface.

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.

**Bypass NIC**

Under normal circumstances, you can have a one- to three-second loss of connection when the device switches to bypass mode, and an 18-second loss when it switches out. Being connected to certain switches, such as some models of Cisco Catalyst, can change these numbers. In this case, you can have a 33-second loss of connection when the device switches to bypass mode and when it switches out.
If you have the scenario where it takes 33 seconds to reestablish communications, you can enable port fast on the switch port and manually set the speed and duplex to get the times back to normal. Be sure to set all four ports (switch, both on Nitro IPS, and other device) to the same setting or you might have a negotiation problem in bypass mode.

The available bypass options depend on the type of bypass NIC in the device, Type 2 or Type 3.

**Set up bypass NICs**

On IPS devices, you can define bypass NIC settings to allow all traffic to pass through.

ADM and DEM devices are always in IDS mode. You can view their bypass NIC type and status but you can’t change their settings.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the **Properties** icon.
2. Click **Configuration** | **Interfaces**.
3. On the **Network Interface Settings** page, go to the **Bypass NIC Configuration** section at the bottom.
4. View the type and status or, on an IPS, change the settings.
5. Click **OK**.

**Add VLANs and aliases**

Add Virtual Local Area Networks (VLANs) and aliases (assigned IP address and netmask pairs that you add if you have a network device that has more than one IP address) to an ACE or ELM interface.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the **Properties** icon.
2. Click device **Configuration**, click **Interfaces**, then click **Advanced**.
3. Click **Add VLAN**, enter the information requested, then click **OK**.
4. Select the VLAN you want to add the alias to, then click **Add Alias**.
5. Enter the information requested, then click **OK**.

**Configure SNMP notifications**

To configure device-generated SNMP notifications, you must define which traps should be sent and their destinations.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the **Properties** icon.
2. Click **Configuration** | **SNMP**.
3. Define the settings, then click **OK**.
Set up NTP on a device
Synchronize the device time with the ESM using a Network Time Protocol (NTP) server.

Task
For option definitions, click ? in the interface.

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.

Tasks
- View status of NTP servers on page 155
  View the status of all the NTP servers on the ESM.

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

Task
For option definitions, click ? in the interface.

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

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

Task
For option definitions, click ? in the interface.

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

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

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

⚠️ The device does not send an event to the ELM until after its aggregation time period has expired.
Task
For option definitions, click ? in the interface.

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

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

General device information and settings
Each device has a page that gives general information about the device, such as serial number and software version. You can also define settings for the device like selecting the zone and syncing the clock.

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

Task
For option definitions, click ? in the interface.

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

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

Update the software on a device
If the software on your device is out of date, upload a new version of the software from a file on the ESM or your local computer.

Before you begin
If you've had your system for more than 30 days, you must obtain and install your permanent credentials to access the updates (see Obtain and add rule update credentials).

⚠️ If you must comply with Common Criteria and FIPS regulations, do not update the ESM in this way. Call McAfee support to obtain a certified update.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click device Management | Update Device.
3. Select an update from the table or click Browse to locate it on your local system.

The device restarts with the updated software version.

**Enter Linux commands for a device**
Use the Terminal option to enter Linux commands on a device. This feature is for advanced users and must be used under the direction of McAfee support personnel for an emergency.

This option is not FIPS-compliant and is disabled in FIPS mode.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click device Management | Terminal.
3. Enter the system password, then click OK.
4. Enter the Linux commands, export the file, or transfer files.
5. Click Close.

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click device Management | Connect.
   
   The button changes to Disconnect and your IP address is provided.
3. Give the IP address to the technical support engineer.
   
   You might need to provide additional information, such as the password.
4. Click Disconnect to end the connection.

**Monitor traffic**
If you need to monitor traffic flowing through a DEM, ADM, or IPS device, you can use TCP Dump to download an instance of the Linux program running on the device.
**Task**  
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the **Properties** icon.
2. Click device **Management**.
3. In the **TCP Dump** section of the page, perform the steps to download the instance.

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

**Task**  
For option definitions, click ? in the interface.

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

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

**Task**  
For option definitions, click ? in the interface.

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

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

**Task**  
For option definitions, click ? in the interface.

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

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

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

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

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

**Task**
For option definitions, click ? in the interface.

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

**Events, flows, and logs**
IPS, ADM, and Receiver devices collect events, flows, and logs; ACE and DEM devices collect events and logs; and ELM devices collect logs. Set each device to check for them manually or automatically. In addition, you can aggregate the events or flows generated by a device.

**Set up events, flows, and logs downloads**
Check for events, flows, and logs manually or set the device to check for them automatically.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Events, Flows & Logs, Events & Logs, or Logs.
3. Set up the downloads, then click Apply.

**Define geolocation and ASN settings**
Geolocation provides the real-world geographic location of computers connected to the Internet. Autonomous System Number (ASN) is a number that is assigned to an autonomous system and uniquely identifies each network on the Internet.

Both of these types of data can help you identify the physical location of a threat. Source and destination geolocation data can be collected for events.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.

2. Click Events, Flows & Logs or Events & Logs, then click Geolocation.

3. Make the selections to generate the information needed, then click OK.

You can filter event data using this information.

**Aggregating events or flows**
An event or flow can potentially be generated thousands of times. Instead of forcing you to sift through thousands of identical events, aggregation allows you to view them as a single event or flow with a count that indicates the number of times it occurred.

Using aggregation uses disk space on both the device and ESM more efficiently because it eliminates the need to store each packet. This feature applies only to rules that have aggregation enabled in the Policy Editor.

**Source IP and destination IP address**
The source IP 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:FF:0000: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 ten minutes after noon, the First time field contains the time 12:00 (the time of the first instance of the event), the Last time field contains the time 12:10 (the time of the last instance of the event), and the Total field contains the value 30.

You can change the default event or flow aggregation settings for the device as a whole and, for events, you can add exceptions to the device's settings for individual rules (see Manage event aggregation exceptions).

Dynamic aggregation is also enabled by default. When it is selected, it replaces the settings for Level 1 aggregation and increases the settings for Level 2 and Level 3. It 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 that it is pulled by the ESM. 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 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 privileges to change these settings.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Event Aggregation or Flow Aggregation.
3. Define the settings, then click OK.

Manage event aggregation exceptions
You can view a list of the event aggregation exceptions that were added to the system. You can also edit or remove an exception.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Event Aggregation, then click View at the bottom of the screen.
3. Make the needed changes, then click Close.

Add exceptions to event aggregation settings
Aggregation settings apply to all events generated by a device. You can create exceptions for individual rules if the general settings don't apply to the events generated by that rule.

**Task**
For option definitions, click ? in the interface.

1. On the views pane, select an event generated by the rule you want to add an exception for.
2. Click the Menu icon, then select Modify Aggregation Settings.
3. Select the field types you want to aggregate from the Field 2 and Field 3 drop-down lists.

The fields you select in Field 2 and Field 3 must be different types or an error results. When you select these field types, the description for each aggregation level changes to reflect the selections you made. The time limits for each level depend on the event aggregation setting you defined for the device.

4. Click OK to save your settings, then click Yes to proceed.
5. Deselect devices if you do not want to roll out the changes to them.
6. Click OK to roll out the changes to the devices that are selected.
The **Status** column shows the status of the update as the changes are rolled out.

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

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

**Maximum number of devices per model**
The number of virtual devices that can be added to an ADM or Nitro IPS is based on the model:

<table>
<thead>
<tr>
<th>Device maximum</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>APM-1225</td>
</tr>
<tr>
<td></td>
<td>NTP-1225</td>
</tr>
<tr>
<td></td>
<td>APM-1250</td>
</tr>
<tr>
<td></td>
<td>NTP-1250</td>
</tr>
<tr>
<td>4</td>
<td>APM-2230</td>
</tr>
<tr>
<td></td>
<td>NTP-2230</td>
</tr>
<tr>
<td></td>
<td>NTP-2600</td>
</tr>
<tr>
<td></td>
<td>APM-3450</td>
</tr>
<tr>
<td></td>
<td>NTP-3450</td>
</tr>
<tr>
<td>8</td>
<td>NTP-2250</td>
</tr>
<tr>
<td></td>
<td>NTP-4245</td>
</tr>
<tr>
<td></td>
<td>NTP-5400</td>
</tr>
<tr>
<td>0</td>
<td>APM-VM</td>
</tr>
<tr>
<td></td>
<td>NTP-VM</td>
</tr>
</tbody>
</table>

**How selection rules are used**
Selection rules are used as filters to determine which packets are processed by a virtual device.

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, it is processed by the virtual device that contains the matching selection rule. Otherwise it is passed on to the next virtual device in order, then is processed by the ADM or Nitro IPS itself, as a default, if no selection rules are matched on any virtual devices.
Things to note for IPv4 virtual devices:

- All packets for a single connection are sorted based only on the first packet in the connection. If the first packet in a connection matches a selection rule for the third virtual device in the list, all subsequent packets in that connection go to the third virtual device, even if the packets match a virtual device that is higher in the list.

- Invalid packets (a packet that is not setting up a connection or part of an established connection) are sorted to the base device. For example, you have a virtual device that is looking for packets with a source or destination port of 80. When an invalid packet comes through with a source or destination port of 80, it is sorted to the base device instead of the virtual device that looks for port 80 traffic. Therefore, you see events in the base device that look like they should have gone to a virtual device.

The order that selection rules are listed is important because the first time a packet matches a rule, that packet is automatically routed to that virtual device for processing. For example, you add four selection rules and the fourth one in order is the filter that triggers most often. This means the other filters for this virtual device must be passed over by each packet 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 order in which virtual devices are checked is important because the packets coming into the ADM or Nitro IPS device are compared to the selection rules for each virtual device in the order that the virtual devices are set up. The packet makes it to the selection rules for the second virtual device only if it doesn't match any selection rules on the first device.

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

- To change the order on a Nitro IPS device, use the arrows on the Virtual Devices page (IPS Properties | Virtual Devices).

**ADM virtual devices**

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

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

**Manage selection rules**

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

The order that selection rules are listed in is important because the first time a packet matches a rule, that packet is automatically routed to that virtual device for processing.
Task
For option definitions, click ? in the interface.

1 Select an IPS or ADM device node, then click the Properties icon.
2 Click Virtual Devices, then click Add.
   The Add Virtual Device window opens.
3 Add, edit, remove, or change the order of the selection rules in the table.

Add a virtual device
You can add a virtual device to some ADM and IPS devices, setting the selection rules that determine which packets are processed by each device.

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

Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select an ADM or IPS device, then click the Properties icon.
2 Click Virtual Devices | Add.
3 Enter the information requested, then click OK.
4 Click Write to add the settings to the device.

Manage custom display types
You can define how you want the devices on the system navigation tree to be organized by adding, editing, or deleting custom display types.

Task
For option definitions, click ? in the interface.

1 On the system navigation pane, click the display type drop-down arrow.
2 Do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a custom display type</td>
<td>1 Click Add Display.</td>
</tr>
<tr>
<td></td>
<td>2 Fill in the fields, then click OK.</td>
</tr>
<tr>
<td>Edit a custom display type</td>
<td>1 Click the Edit icon next to the display type you want to edit.</td>
</tr>
<tr>
<td></td>
<td>2 Make changes to the settings, then click OK.</td>
</tr>
<tr>
<td>Delete a custom display type</td>
<td>Click the Delete icon next to the display type you want to delete.</td>
</tr>
</tbody>
</table>
Select a display type
Select the way you want to display the devices in the system navigation tree.

Before you begin
To select a custom display, you must add it to the system first (see Manage 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 organization of the devices on the navigation tree changes to reflect the type you selected for the current work session.

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

Before you begin
Add a custom display type (see Manage custom display types).

Task
For option definitions, click ? in the interface.
1. On the system navigation pane, click the display type drop-down list.
2. Select the custom display, then do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Add a new group  | 1. Click a system or group node, then click the Add Group icon on the actions toolbar.  
|                  | 2. Fill in the fields, then click OK.                                      |
|                  | 3. Drag-and-drop devices on the display to add them to the group.          |
|                  |   If the device is part of a tree on the display, a duplicate device node is created. You can then delete the duplicate on the system tree. |
| Edit a group     | Select the group, click the Properties icon, then make changes on the Group Properties page. |
| Delete a group   | Select the group, then click the Delete Group icon. The group and the devices that are in it are deleted from the custom display. The devices are not deleted from the system. |

See also
Manage custom display types on page 24

Delete duplicate devices on the system navigation tree
Duplicate device nodes can appear on the system navigation tree when you drag and drop devices from a system tree into a group or when you have groups set up and then upgrade the ESM software. We recommend that you delete them to avoid confusion.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation pane, click the display type drop-down list.

2. Select the **Edit** icon next to the display that includes the duplicate devices.

3. Deselect the duplicate devices, then click **OK**.

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

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select the devices you want to manage.

2. Click the **Multi-Device Management** icon on the actions toolbar.

3. Select the operation you want to perform and the devices you want to perform it on, then click **Start**.

**Manage URL links for all devices**
You can set up a link for each device to view device information on a URL.

**Before you begin**
Set up the URL site for the device.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Custom Settings | Device Links**.

2. To add or edit a URL, highlight the device, click **Edit**, then enter the URL.
   The URL field has a limit of 512 characters.

3. Click **OK**.

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

**View device summary reports**
The device summary reports show the types and number of devices on the ESM and the last time an event was received by each one. These reports can be exported in comma-separated value (CSV) format.
**Task**
For option definitions, click ? in the interface.

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

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

**Task**
For option definitions, click ? in the interface.

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

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

**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
A flag on this type of node... Opens...

<table>
<thead>
<tr>
<th>System or group</th>
<th>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:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition deleted</td>
<td>A database table containing the event, flow, or log data has reached its maximum size and has deleted a partition to add space for new records. Event, flow, and log data can be exported to avoid permanent loss.</td>
</tr>
<tr>
<td>Drive Space</td>
<td>A hard drive is full or running low on space. This could include the hard drive on the ESM, redundant ESM, or remote mount point.</td>
</tr>
<tr>
<td>Critical</td>
<td>The device is not working properly and should be fixed.</td>
</tr>
<tr>
<td>Warning</td>
<td>Something on the device is not functioning the way it should.</td>
</tr>
<tr>
<td>Informational</td>
<td>The device is working properly but the device status level changed.</td>
</tr>
<tr>
<td>Out of Sync</td>
<td>The virtual device, data source, or database server settings on the ESM are out of sync with what is actually on the device.</td>
</tr>
<tr>
<td>Rolled over</td>
<td>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.</td>
</tr>
<tr>
<td>Inactive</td>
<td>The device has not generated events or flows within the inactivity threshold time period.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The ESM couldn't connect to the device.</td>
</tr>
</tbody>
</table>

Partition deleted, Drive space, Rolled over, and Informational flags can be cleared by checking the boxes next to the flags and clicking Clear Selected or Clear All.

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 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 time 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.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description and instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypass mode</td>
<td>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</td>
</tr>
<tr>
<td>Deep Packet Inspector not running</td>
<td>The Deep Packet Inspector (DPI) has malfunctioned. It might recover without intervention. If not, restart the device.</td>
</tr>
<tr>
<td>Firewall alert program (ngulogd) not running</td>
<td>The Firewall Alert Aggregator (FAA) has malfunctioned. It might recover without intervention. If not, restart the device.</td>
</tr>
<tr>
<td>Database not running</td>
<td>The McAfee Extreme Database (EDB) server has malfunctioned. Restarting the device might solve the problem, but the database might need to rebuild.</td>
</tr>
<tr>
<td>Status</td>
<td>Description and instructions</td>
</tr>
<tr>
<td>--------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Oversubscription mode</td>
<td>If the monitored network is busier than Nitro IPS can handle, network packets might not be inspected. The health monitor generates an alert indicating that the Nitro IPS is oversubscribed. By default, the oversubscription mode value is set to drop. To change the value, navigate to Policy Editor, click Variable in the Rule Types pane, expand the packet_inspection variable, and select Inherit for the OVERSUBSCRIPTION_MODE variable. Pass and Drop are allowed for this variable.</td>
</tr>
<tr>
<td>Control channel not running</td>
<td>The process that services the communication channel with the ESM has failed. A device reboot might remedy the problem.</td>
</tr>
<tr>
<td>RDEP or Syslog programs not running</td>
<td>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.</td>
</tr>
<tr>
<td>Health Monitor unable to communicate with the Deep Packet Inspector controller program</td>
<td>The Health Monitor is unable to communicate with the Deep Packet Inspector to retrieve its status. This could mean that the control program is not running and network traffic might not be passing through the Nitro IPS. Reapplying the policy might resolve the issue.</td>
</tr>
<tr>
<td>System logger not running</td>
<td>The system logger is not responding. A reboot of the device might remedy the problem.</td>
</tr>
<tr>
<td>Hard drive partition free space low</td>
<td>The amount of free disk space is critically low.</td>
</tr>
<tr>
<td>Fan speed alert</td>
<td>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.</td>
</tr>
<tr>
<td>Temperature Alert</td>
<td>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.</td>
</tr>
<tr>
<td>Network errors</td>
<td>There are network errors or excessive collisions on the network. The cause might be a large collision domain or bad network cables.</td>
</tr>
<tr>
<td>Problem with a remote mount point</td>
<td>There is a problem with a remote mount point.</td>
</tr>
<tr>
<td>Remote mount point free disk space low</td>
<td>The remote mount point free disk space is low.</td>
</tr>
<tr>
<td>All data source collectors that have not received communication from a data source for at least 10 minutes</td>
<td>The Receiver has not received any communication from a data source for at least 10 minutes.</td>
</tr>
<tr>
<td>Data source collector not running</td>
<td>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.</td>
</tr>
<tr>
<td>Health Monitor unable to get a valid status from a subsystem</td>
<td>The health monitor was unable to get a valid status from a subsystem.</td>
</tr>
<tr>
<td>Subsystem recovery from a warning or critical status</td>
<td>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.</td>
</tr>
</tbody>
</table>
Delete a group or device
When a device is no longer part of the system or you no longer use a group, delete it from the system navigation tree.

Task
For option definitions, click ? in the interface.

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

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

• On the actions toolbar, click the Refresh Devices icon.

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

Contents

▶ Devices and what they do
▶ Event Receiver settings
▶ Enterprise Log Manager (ELM) settings
▶ Advanced Correlation Engine (ACE) settings
▶ Application Data Monitor (ADM) settings
▶ Database Event Monitor (DEM) settings
▶ Distributed ESM (DESM) settings
▶ ePolicy Orchestrator settings
▶ Nitro Intrusion Prevention System (Nitro IPS) settings
▶ McAfee Vulnerability Manager settings
▶ McAfee Network Security Manager settings
**Devices and what they do**

The ESM enables you to administer, manage, and interact with all physical and virtual devices in your security environment.

**See also**

- Event Receiver settings on page 55
- Enterprise Log Manager (ELM) settings on page 103
- Application Data Monitor (ADM) settings on page 120
- Database Event Monitor (DEM) settings on page 134
- Advanced Correlation Engine (ACE) settings on page 117
- Distributed ESM (DESM) settings on page 141
- ePolicy Orchestrator settings on page 141
- Nitro Intrusion Prevention System (Nitro IPS) settings on page 147
Event Receiver settings
The Event Receiver enables the collection of security events and network flow data from multi-vendor sources including firewalls, virtual private networks (VPNs), routers, Nitro IPS/IDS, NetFlow, sFlow, and others.

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

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

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

Task
For option definitions, click ? in the interface.

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.

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

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

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

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

These Receiver models can be purchased with High Availability function:

• ERC-1225-HA
• ERC-2230-HA
• ERC-2250-HA
• ERC-1250-HA
• ERC-1260-HA
• ERC-2600-HA
These models include an Intelligent Platform Management Interface (IPMI) port as well as at least 4 NICs, which are necessary for HA functionality (see Network ports on Receiver-HA).

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

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

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

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

**Primary Receiver failure**

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

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

**Secondary Receiver failure**

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

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

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

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

Secondary health problem

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

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

Returning to service

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

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

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

Upgrading Receiver-HA

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

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

When upgrading, it is best not to have a preferred primary Receiver. Refer to If your Receiver-HA is set up with a preferred primary, it is best to change the setting before upgrading. On the HA Receiver tab (see Set up Receiver-HA Devices), select None in the Preferred primary device field. This allows you to use the Fail-over option, which is not available with a preferred primary setting. After both Receivers are upgraded, you can apply the preferred primary setting again.
Network ports on Receiver-HAs
These diagrams show how to connect the network ports on a Receiver-HA.

**ERC-1250-HA/1260-HA**

1. IPMI
2. Mgmt 2
3. Mgmt 1
4. IPMI NIC
5. Heart beat (HB)
6. Mgmt 2
7. Mgmt 3
8. Data feed
9. Mgmt 1 IP

**ERC-2600-HA and ERC-4600-HA**
Set up Receiver-HA Devices
Define the settings for the Receiver-HA devices.

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

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select the Receiver that will be the primary HA device, then click the Properties icon.
2. Click Receiver Configuration, then click Interface.
3 Click the HA Receiver tab, then select Setup High Availability.

4 Fill in the information requested, then click OK.

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

**Reinitialize the secondary device**

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

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, select Receiver Properties for the primary Receiver, then click Receiver Configuration | Interface | HA Receiver.

2 Verify that the correct IP address is in the Secondary Management IP field.

3 Click Reinitialize Secondary.

The ESM performs the necessary steps to reinitialize the Receiver.

**Reset HA devices**

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

- Do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset a Receiver on the ESM console</td>
<td>1 On the system navigation tree, click Receiver Properties, then click Receiver Configuration</td>
</tr>
<tr>
<td></td>
<td>2 Deselect Setup High Availability, then click OK.</td>
</tr>
<tr>
<td></td>
<td>3 Click Yes on the warning page, then click Close.</td>
</tr>
<tr>
<td></td>
<td>Both Receivers restart after a timeout of about five minutes, returning the MAC addresses to their original values.</td>
</tr>
<tr>
<td>Reset the primary or secondary Receiver on the LCD menu</td>
<td>1 On the Receiver’s LCD menu, press X.</td>
</tr>
<tr>
<td></td>
<td>2 Press the down arrow until you see Disable HA.</td>
</tr>
<tr>
<td></td>
<td>3 Press the right arrow once to display Disable Primary on the LCD screen.</td>
</tr>
<tr>
<td></td>
<td>4 To reset the primary Receiver, press the checkmark.</td>
</tr>
<tr>
<td></td>
<td>5 To reset the secondary Receiver, press the down arrow once, then press the checkmark.</td>
</tr>
</tbody>
</table>

**Switch Receiver-HA roles**

The user-initiated switch-over process allows you to switch the roles of the primary and secondary Receivers.

You might need to do this when upgrading a Receiver, preparing a Receiver to be returned to the manufacturer, or moving cables on a Receiver. This switch minimizes the amount of data lost.

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

1. On the system navigation tree, select the Receiver-HA device, then click the Properties icon.

2. Select High Availability | Fail-Over. The following happens:
   - The ESM instructs the secondary Receiver to start using the shared data source IP and collecting data.
   - The secondary Receiver issues a Cluster Resource Manager (CRM) command to switch the shared IP and MAC, and starts the collectors.
   - The ESM pulls all alert and flow data from the primary Receiver.
   - The ESM marks the secondary Receiver as the primary and marks the primary Receiver as the secondary.

Upgrade HA Receivers
The Receiver-HA upgrade process upgrades both Receivers sequentially, starting with the secondary Receiver.

Before starting the upgrade process, go through the Check Receiver high availability status process to make sure that the Receiver-HA devices are ready to be upgraded. Failure to do so can result in problems with the device upgrade and downtime.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the Receiver-HA device, then click the Properties icon.

2. Upgrade the secondary Receiver:
   a. Click Receiver Management, then select Secondary.
   b. Click Update Device, then select or browse to the file you want to use and click OK.
      The Receiver restarts and the version of software is updated.
   c. On Receiver Properties, click High Availability | Return to Service.
   d. Select the secondary Receiver, then click OK.

3. Change the secondary Receiver to primary by clicking High Availability | Fail-Over.

4. Upgrade the new secondary Receiver by repeating step 2.

Check Receiver high availability status
Determine the status of an HA Receiver pair prior to performing an upgrade.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the primary Receiver-HA device, then click the Properties icon.

2. In the Status and Secondary Status fields, verify that the status is OK; HA Status: online.
3 Secure shell, or SSH, to each of the HA Receivers and run the `ha_status` command from the command-line interface on both Receivers. The resulting information shows the status of this Receiver and what this Receiver thinks the status of the other Receiver is. It looks similar to this:

```
OK

hostname=McAfee1
mode=primary
McAfee1=online
McAfee2=online
sharedIP=McAfee1
stonith=McAfee2
corosync=running
hi_bit=no
```

4 Verify the following in the above:
   - The first line of the response is `OK`.
   - **Hostname** is the same as the host name on the command line minus the Receiver model number.
   - **Mode** is primary if the value of `sharedIP` is this Receiver's host name; otherwise the mode is secondary.
   - The next two lines show the host names of the Receivers in the HA pair and list the running status of each Receiver. The status for both is `online`.
   - `corosync=` shows the running status of corosync, which should be running.
   - `hi_bit` is `no` on one Receiver and `yes` on the other Receiver. It doesn't matter which one is which.

   Make sure that only one of the HA Receivers is set with the hi_bit value. If both HA Receivers are set to the same value you should call McAfee Support before doing the upgrade to correct this misconfigured setting.

5 Secure shell, or SSH, to each of the HA Receivers and run the `ifconfig` command from the command-line interface of both Receivers.

6 Verify the following in the data that is generated:
   - The MAC addresses on eth0 and eth1 are unique on both Receivers.
   - The primary Receiver has the shared IP address on eth1 and the secondary Receiver has no IP address on eth1.
     If both HA Receivers are set to the same value, call McAfee support before upgrading to correct this misconfigured setting.

This spot check ensures the system is functional and that no duplication of IP addresses exists, which means that the devices can be upgraded.
Replace a failed Receiver

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

Task

For option definitions, click ? in the interface.

1. On the system navigation tree, select Receiver Properties for the HA Receiver, then click Receiver Configuration | Interface.

2. Click the HA Receiver tab, then verify that Setup High Availability is selected.

3. Verify that the IP addresses are correct, then click Reinitialize Secondary.

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

Troubleshooting failed Receiver

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

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

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

Archiving Receiver raw data

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

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

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

Define archive settings

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

For option definitions, click ? in the interface.

1. On the system navigation tree, select **Receiver Properties**, then click **Receiver Configuration** | **Data Archival**.

2. Select the share type and enter the information requested.

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

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

**View source events for correlation event**

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

### Before you begin

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, expand the Receiver, then click **Correlation Engine**.

2. On the view list, click **Event Views**, then select **Event Analysis**.

3. On the **Event Analysis** view, click the plus sign (+) in the first column next to the correlation event.

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

The source events are listed under the correlation event.

**View Receiver throughput statistics**

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

### Before you begin

Verify that you have the Device Management privilege.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a Receiver, then click the Properties icon.

2. Click **Receiver Management** | **View Statistics** | **Throughput**.

3. View the Receiver statistics.

   - If incoming rates exceed the output rate by 15 percent, the system flags that row as either critical (in the last 24 hours) or as a warning (in the last hour).

4. Filter the data source by selecting the All, Critical, or Warning options.
5 Select the unit of measure to display the metrics: by number of kilobytes (KBs) or number of records.

6 To refresh the data automatically every 10 seconds, select the Auto Refresh checkbox.

7 Sort data by clicking the relevant column title.

**Receiver data sources**

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

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

**Add a data source**

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

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, select the Receiver you want to add the data source to, then click the Properties icon.

2 On Receiver Properties, click Data Sources | Add.

3 Select the vendor and the model.

The fields you fill out depend on your selections.

4 Fill in the information requested, then click OK.

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

**Processing data source with SNMP Trap**

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

These standard traps are:

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

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

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

If you select SNMP Trap, there are three options:
• If a profile has not been selected previously, the **SNMP Data Source Profiles** dialog box opens, allowing you to select the profile to be used.

• If a profile has been selected previously, the **SNMP Data Source Profiles** dialog box opens. To change the profile, click the down arrow in the **System Profiles** field and select a new profile.

• If a profile has been selected previously and you want to change it but the drop-down list on the **SNMP Data Source Profiles** dialog box does not include the profile you need, create a data source SNMP profile.

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

**Task**
For option definitions, click ? in the interface.

1  On the system navigation tree, select **Receiver Properties**, then click **Data Sources**.

2  View a list of the data sources on the Receiver and perform any of the available options to manage them.

3  Click **Apply** or **OK**.

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

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

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

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

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

**Integrating vulnerability assessment data**
Vulnerability Assessment (VA) on the DEM and Receiver allows you to integrate data that can be retrieved from many VA vendors.
You can use this data in several ways.
• Raise an event’s severity based on the endpoint’s known vulnerability to that event.
• Set the system to automatically learn assets and their attributes (operating system and services detected).
• Create and manipulate the membership of user-defined asset groups.
• Access summary and drill-down information of the network assets.
• Modify Policy Editor configuration such as turn on MySQL signatures if an asset is discovered running MySQL.

You can access VA data generated by the system on predefined views or on custom views that you create. The predefined views are:
• Dashboard Views | Asset Vulnerability Dashboard
• Compliance Views | PCI | Test Security Systems and Processes | 11.2 Network Vulnerability Scans
• Executive Views | Critical Vuln on Regulated Assets

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

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

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

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

Task
For option definitions, click ? in the interface.

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.

Add a VA source
To communicate with VA sources, you must add the source to the system, configure communication parameters for the VA vendor, schedule parameters to dictate how often data is retrieved, and modify event severity calculations.

Task
For option definitions, click ? in the interface.

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

Click Apply or OK.

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

Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select DEM or Receiver Properties, then click Vulnerability Assessment.

2 Select the VA source, then select one of these options.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrieve immediately</td>
<td>• Click Retrieve.</td>
</tr>
<tr>
<td></td>
<td>The job runs in the background and you are informed if the retrieval is successful (see Troubleshoot VA retrieval if it is not successful).</td>
</tr>
<tr>
<td>Schedule retrieval</td>
<td>1 Click Edit.</td>
</tr>
<tr>
<td></td>
<td>2 In the Schedule VA data retrieval field, select the frequency.</td>
</tr>
<tr>
<td></td>
<td>3 Click OK.</td>
</tr>
<tr>
<td></td>
<td>4 On the Vulnerability Assessment page, click Write to write the changes to the device.</td>
</tr>
</tbody>
</table>

3 Click OK.

4 To view the data, click the Asset Manager quick launch icon, then select the Vulnerability Assessment tab.

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

<table>
<thead>
<tr>
<th>This resource...</th>
<th>Causes...</th>
</tr>
</thead>
</table>
| 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; therefore, when you perform a VA retrieval, no data is returned because it's perceived as old data. To avoid this situation, either delete the old Nessus file off of the FTP site before uploading the new one, or use a different name for the file you upload. |
Available VA vendors
The ESM can integrate with these VA vendors.

<table>
<thead>
<tr>
<th>VA vendor</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digital Defense Frontline</td>
<td>5.1.1.4</td>
</tr>
<tr>
<td>eEye REM (REM events server)</td>
<td>3.7.9.1721</td>
</tr>
<tr>
<td>eEye Retina</td>
<td>5.13.0, Audits: 2400</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>McAfee Vulnerability Manager</td>
<td>6.8, 7.0</td>
</tr>
<tr>
<td>Critical Watch FusionVM</td>
<td>4-2011.6.1.48</td>
</tr>
<tr>
<td>LanGuard</td>
<td>10.2</td>
</tr>
<tr>
<td>Lumension</td>
<td>Support PatchLink Security Management Console 6.4.5 and later</td>
</tr>
<tr>
<td>nCircle</td>
<td>6.8.1.6</td>
</tr>
<tr>
<td>Nessus</td>
<td>Support Tenable Nessus versions 3.2.1.1 and 4.2 and file formats NBE, .nessus (XMLv2), and .nessus (XMLv1); also, OpenNessus 3.2.1 XML format</td>
</tr>
<tr>
<td>NGS</td>
<td></td>
</tr>
<tr>
<td>OpenVAS</td>
<td>3.0, 4.0</td>
</tr>
<tr>
<td>Qualys</td>
<td></td>
</tr>
<tr>
<td>Rapid7 Nexpose</td>
<td></td>
</tr>
<tr>
<td>Rapid7 Metasploit Pro</td>
<td>4.1.4-Update 1, file format XML</td>
</tr>
<tr>
<td>Saint</td>
<td></td>
</tr>
</tbody>
</table>

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

Before you begin
Ensure that auto check is selected on the Events, Flows & Logs dialog (System Properties | Events, Flows & Logs) or click the Get Events and Flows icon on the actions toolbar to pull events and/or flows.
Task
For option definitions, click ? in the interface.

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

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

Task
For option definitions, click ? in the interface.

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

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

Set the date format for data sources
Select the format for dates included in data sources.

Task
For option definitions, click ? in the interface.

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

Out-of-sync data sources
As a result of several possible settings, the time on a data source can get out of sync with the ESM. When an out-of-sync data source generates an event, a red flag appears next to the Receiver on the system navigation tree.

You can set up an alarm to notify you when this occurs. You can then manage the data sources that are out of sync by accessing the Time Delta page (see Manage out-of-sync data sources).

Out-of-sync events can be old events or future events.

There are several reasons your data sources can be out of sync with the ESM.
1. The ESM has the incorrect time zone setting (see Select user settings).
2. You set the time to the wrong zone when adding the data source (see Add a data source).
3. The system has been on for a long time and the timing slips out of sync.
4. You set up the system that way on purpose.
5. The system isn’t connected to the Internet.
6. The event is out of sync when it comes in to the Receiver.

See also
Add a data source on page 65
Manage out-of-sync data sources on page 71
Select user settings on page 27

Manage out-of-sync data sources
If you have data sources that are out of sync with the ESM, you can set up an alarm to notify you when events are generated by these data sources. You can then view a list of the data sources, edit their settings, and export this list.

Task
For option definitions, click ? in the interface.

1. Set up an alarm to notify you when an event comes in to the Receiver, generated by a data source that is out of sync with the ESM.
   a. On the system navigation tree, select the system, then click the Properties icon.
   b. Click Alarms | Add, type the information requested on the Summary tab, then click the Condition tab.
   c. Select Event Delta in the Type field, select how often the ESM should check for out-of-sync data sources, and select the time difference that must exist for the alarm to trigger.
   d. Complete the information in the remaining tabs.
2. View, edit, or export the data sources that are out of sync.
   a. On the system navigation tree, click the Receiver, then click the Properties icon.
   b. Click Receiver Management, then click Time Delta.

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

Task
For option definitions, click ? in the interface.

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

The data source is added as a child below the parent data source on the table and on the system navigation tree.
**Client data sources**
You can extend the number of data sources allowed on a Receiver by adding client data sources. For data sources with a syslog, ASP, CEF, MEF, NPP, and WMI collector, you can add up to 65,534 data source clients.

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

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

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

Client data sources have these characteristics:

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

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

**Add a client data source**
Add a client to an existing data source to increase the number of data sources allowed on the Receiver.

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **Receiver Properties**, then click **Data Sources**.
2. Select the data source that you want to add the client to, then click **Clients**.
   
The **Data source clients** page lists the clients that are currently part of the selected data source.
3. Click **Add**, fill in the information requested, then click **OK**.

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

**Locate a client**
The **Data source clients** page lists all the clients on the system. Because you can have more than 65,000 clients, a search feature is provided so that you can locate a specific one, if needed.
**Task**  
For option definitions, click ? in the interface.

1. On the system navigation tree, select **Receiver Properties**, then click **Data Sources | Clients**.

2. Enter the information you want to search for, then click **Search**.

**Import a list of data sources**

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

There are two situations in which you use this option:

- To import raw data source data copied from a Receiver in a secured location to a Receiver in an unsecured location. If this is what you are doing, see **Move data sources**.

- To edit the data sources on a Receiver by adding data sources to the existing list, editing existing data sources, or removing existing data sources. If this is what you need to do, follow these steps.

**Task**  
For option definitions, click ? in the interface.

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

2. The list of existing data sources is saved.

   a. Access and open this file.

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

2. Add, edit, or remove data sources on the list.
   a. In column A, specify the action to be taken with that data source: add, edit, or remove.

   b. If you are adding or editing data sources, enter the information in the spreadsheet columns.

   ![Tip](You can't edit the policy or the name of the data source.)

   c. Save the changes made to the spreadsheet.

   ![Tip](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**.

   ![Tip](You can't change the policy or the name of the data source)

   The **Import Data Sources** page opens, listing the changes that have been made to the spreadsheet.
c To import the changes, click OK.
   The changes that are formatted correctly are added.

d If there are errors in the formatting of the changes, a **Message Log** describes the errors.

e Click **Download Entire File**, then click **Yes**.

f Select the location for the download to be saved, change the name of the file if needed, then click **Save**.

g Open the file that downloaded.
   It lists the data sources that have errors.

h Correct the errors, then save and close the file.

i Close **Message Log** and **Import Data Sources**, then click **Import** and select the file that you saved.
   **Import Data Sources** lists the data sources that you corrected.

j Click **OK**.

**Spreadsheet fields for importing data sources**
The spreadsheet you use to import data sources has several columns; some are required and some are used only for specific data source types.

**Fields required for all data sources**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
</table>
| op     | Operation to be performed on the data source | Enter one of these functions in the `op` column:
|        |                                      | • **add** = Add a data source.
|        |                                      | • **edit** = Modify an existing data source.
|        |                                      | • **remove** = Remove without reassigning.
|        |                                      | If this column is left blank, no action is taken on the data source. |
| rec_id | Receiver ID                          | This Device ID number can be found on the Receiver's **Name and Description** page. |
| dsname | Name for the data source             | Must be unique on the Receiver. |
### Fields used by all data sources

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip</td>
<td>Valid IP address for the data source</td>
<td>• It is required except if the protocol = 'corr'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Validation is performed for enabled data sources only. Excludes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protocols: cifs, nfs, ftp, scp, http</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Collector = 'curl' or 'mount'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SNMPTrap - Not valid if other data sources use SNMP trap and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP Address matches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• nfsql - Not valid if combination of IP Address, 'dbname', and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>'port' found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• netflow or opsec - Not valid if combination of IP Address and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>'port' found.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• mef is the collector (if parser is mef, collector is automatically</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mef) - Not valid if mef and protocol are found.</td>
</tr>
<tr>
<td>model</td>
<td></td>
<td>Entry must be an exact match, except for clients with MatchByFlag</td>
</tr>
<tr>
<td></td>
<td></td>
<td>= 1 (match by IP Address)</td>
</tr>
<tr>
<td>vendor</td>
<td></td>
<td>Entry must be an exact match, except for clients with MatchByFlag</td>
</tr>
<tr>
<td></td>
<td></td>
<td>= 1 (match by IP Address)</td>
</tr>
<tr>
<td>parent_id</td>
<td>ID of the parent data source</td>
<td>Required if it's an agent or client. If this ID is a name, an attempt</td>
</tr>
<tr>
<td></td>
<td></td>
<td>is made to find the data source parent with this name that is a</td>
</tr>
<tr>
<td></td>
<td></td>
<td>child of the specified Receiver.</td>
</tr>
<tr>
<td>child_type</td>
<td>Type of data source child</td>
<td>Required: 0 = not a child, 1 = agent, 2 = client</td>
</tr>
<tr>
<td>match_type</td>
<td>Client matching</td>
<td>Required when adding or editing data sources: 1 = match by IP address,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = match by third-party type</td>
</tr>
<tr>
<td>parsing</td>
<td>Data source enabled flag</td>
<td>Enabled flag (yes/no), default is yes</td>
</tr>
</tbody>
</table>

### Fields used by data sources that are not clients

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp_trap_id</td>
<td>Profile ID for snmp trap</td>
<td>Default is 0.</td>
</tr>
<tr>
<td>elm_logging</td>
<td>Log to elm (yes/no)</td>
<td>Default is no.</td>
</tr>
<tr>
<td>pool</td>
<td>Elm pool name</td>
<td>Default is blank.</td>
</tr>
<tr>
<td>meta-vendor</td>
<td></td>
<td>Default is blank.</td>
</tr>
<tr>
<td>meta-product</td>
<td></td>
<td>Default is blank.</td>
</tr>
<tr>
<td>meta_version</td>
<td></td>
<td>Default is blank.</td>
</tr>
<tr>
<td>url</td>
<td>Event details URL</td>
<td>Default is blank.</td>
</tr>
<tr>
<td>parser</td>
<td>Data format parsing method</td>
<td>Default is Default.</td>
</tr>
<tr>
<td>collector</td>
<td>Data retrieval method</td>
<td>Default is Default. If parser is mef, collector is set to mef. Scp,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>http, ftp, nfs, cifs are okay if flat file format is supported for the protocol.</td>
</tr>
</tbody>
</table>
### Fields required if the format is CEF or MEF

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>encrypt</td>
<td>Data source encryption flag</td>
<td>Default is F. Also used if Format is Default, Retrieval is mef, and Protocol is gsyslog. Encryption must be the same for all mef with same IP address.</td>
</tr>
<tr>
<td>hostname</td>
<td>Host name or host ID</td>
<td>Default is blank. Optional if Protocol is gsyslog or syslog — Must be unique. Optional if Protocol is nas.</td>
</tr>
<tr>
<td>aggregate</td>
<td>Syslog relay</td>
<td>Valid values are blank and syslogng. Default is blank. Also used if Format is Default, Retrieval is Default, and Protocol is gsyslog.</td>
</tr>
<tr>
<td>tz_id</td>
<td>Time zone ID</td>
<td>Default is blank. Also used if Format is Default and one of the following is true:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protocol is syslog and Model is not Adiscon Windows Events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protocol is nfsql.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protocol is nfhttp.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protocol is email.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protocol is estream. Also used for some flat file support</td>
</tr>
</tbody>
</table>

### Other fields

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_id</td>
<td>The profile name or ID</td>
<td>Default is blank. If the profile name cannot find the profile record, an error is logged.</td>
</tr>
<tr>
<td>exportMcAfeeFile</td>
<td>Data source transport flag</td>
<td>Default is no. If yes, this data source is included in data source transport.</td>
</tr>
<tr>
<td>exportProfileID</td>
<td>The remote share profile name</td>
<td>Default is blank.</td>
</tr>
<tr>
<td>mcafee_formated_file</td>
<td>Parse raw data file flag</td>
<td>Default is no. If yes, the parsing method uses the raw data file.</td>
</tr>
<tr>
<td>mcafee_formated_file_xsum</td>
<td>Use check sum flag</td>
<td>Default is no. If yes, use the check sum before parsing the raw data file.</td>
</tr>
<tr>
<td>mcafee_formated_file_ipsid</td>
<td>The original Nitro IPS ID</td>
<td>Required if using the raw data file.</td>
</tr>
<tr>
<td>zoneID</td>
<td>Name of the zone</td>
<td>Default is blank.</td>
</tr>
<tr>
<td>policy_name</td>
<td>Policy name or ID</td>
<td>Default is blank. Used only when adding new data sources. This value is not updated on an edit operation.</td>
</tr>
</tbody>
</table>

### Fields validated for specified protocols

The vendor and model determines the protocol, except when format is Default or CEF, and Retrieval is not Default or MEF. Then the protocol is the Retrieval value. These fields are validated for the specified protocol, if no profile is specified.

### Table 3-2 Netflow Fields — Start at Column AF

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>netflow_port</td>
<td></td>
<td>Default is 9993.</td>
</tr>
<tr>
<td>netflow_repeat_enabled</td>
<td>Forwarding enabled</td>
<td>Default is F.</td>
</tr>
</tbody>
</table>
Table 3-2  Netflow Fields — Start at Column AF (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>netflow_repeat_ip</td>
<td>Forwarding IP address</td>
<td>Required if repeat_enabled = T. Default is blank.</td>
</tr>
<tr>
<td>netflow_repeat_port</td>
<td>Forwarding port</td>
<td>Default is 9996.</td>
</tr>
</tbody>
</table>

Table 3-3  rdep Fields — Start at Column AJ

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdep_sdee_username</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>rdep_sdee_password</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>rdep_sdee_interval</td>
<td>Default is 60 seconds.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-4  opsec Fields — Start at Column AM

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>opsec_parent</td>
<td>Parent flag (device type)</td>
<td>Required (T/F). T = data source is a parent. F = data source is not a parent</td>
</tr>
<tr>
<td>opsec_authentication</td>
<td>Use authentication flag</td>
<td>Used if parent = T, default is F</td>
</tr>
<tr>
<td>opsec_appname</td>
<td>Application name</td>
<td>Required if authentication = T, optional if F, default is blank</td>
</tr>
<tr>
<td>opsec_actkey</td>
<td>Activation key</td>
<td>Required if authentication = T, optional if F, default is blank</td>
</tr>
<tr>
<td>opsec_parent_id</td>
<td>Data source parent name</td>
<td>Parent name - required if parent = F. An error is logged if the data source parent name cannot find the parent data source.</td>
</tr>
<tr>
<td>opsec_port</td>
<td></td>
<td>Used if parent = T, default is 18184</td>
</tr>
<tr>
<td>opsec_encryption</td>
<td>Use encryption flag</td>
<td>Used if parent = T, default is F</td>
</tr>
<tr>
<td>opsec_comm_method</td>
<td>Communication method</td>
<td>Used if parent = T, default is blank. Must be a valid value:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• &quot; (blank)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 'asym_sslca'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 'asym_sslca_comp'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 'asym_sslca_rc4'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 'asym_sslca_rc4_comp'</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 'ssl_clear'</td>
</tr>
<tr>
<td>opsec_server_entity_dn</td>
<td>Server entity</td>
<td>Default is blank. Used if parent = T. Required if DeviceType = Log Server/CLM or Secondary SMS/CMA.</td>
</tr>
<tr>
<td></td>
<td>distinguished name</td>
<td></td>
</tr>
<tr>
<td>opsec_collect_audit_events</td>
<td>Event collection type</td>
<td>Used if parent = T, default is &quot;yes&quot;</td>
</tr>
<tr>
<td></td>
<td>audit events flag</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-4 opsec Fields — Start at Column AM (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>opsec_collect_log_events</td>
<td>Event collection type</td>
<td>Used if parent = T, default is &quot;yes&quot;.</td>
</tr>
<tr>
<td></td>
<td>log events flag</td>
<td></td>
</tr>
<tr>
<td>opsec_type</td>
<td>Device type</td>
<td>Required. Valid values for this field are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Value</strong> Name in thin-client drop-down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0  SMS/CMA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1  Security Device</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2  Log Server/CLM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3  Secondary SMS/CMA</td>
</tr>
</tbody>
</table>

### Table 3-5 wmi Fields — Start at Column AY

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>wmi_use_rpc</td>
<td>Use RPC flag</td>
<td>Default is no.</td>
</tr>
<tr>
<td>wmi_logs</td>
<td>Event logs</td>
<td>Default is SYSTEM, APPLICATION, SECURITY.</td>
</tr>
<tr>
<td>wmi_nbname</td>
<td>NetBIOS name</td>
<td>Required if Retrieval = Default, otherwise optional. Default is blank.</td>
</tr>
<tr>
<td>wmi_username</td>
<td>User name</td>
<td>Required if Retrieval = Default, otherwise optional. Default is blank.</td>
</tr>
<tr>
<td>wmi_password</td>
<td>Password</td>
<td>Required if Retrieval = Default, otherwise optional. Default is blank.</td>
</tr>
<tr>
<td>wmi_interval</td>
<td></td>
<td>Default is 600.</td>
</tr>
<tr>
<td>wmi_version</td>
<td></td>
<td>Default is 0.</td>
</tr>
</tbody>
</table>

### Table 3-6 gsyslog Fields — Start at Column BF

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>gsyslog_autolearn</td>
<td>Support generic syslogs flag</td>
<td>Valid values: T, F, COUNT. Default is F.</td>
</tr>
<tr>
<td>gsyslog_type</td>
<td>Generic rule assignment</td>
<td>Required if autolearn = T; otherwise optional. Default is 49190.</td>
</tr>
<tr>
<td>gsyslog_mask</td>
<td>Used if Retrieval is Default. Default is 0.</td>
<td></td>
</tr>
</tbody>
</table>

### Table 3-7 corr Field — Column BI

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>corr_local</td>
<td>Use local data flag</td>
<td>Default is F. If the Receiver model is ERC-VM-25 or ERC-VM-500, the data source is not added. Otherwise, there can be no other data sources using this Protocol.</td>
</tr>
</tbody>
</table>

### Table 3-8 sdee Fields — Start at Column BJ

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdee_username</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>sdee_password</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>sdee_uri</td>
<td>Default is cgi-bin/sdee-server</td>
<td></td>
</tr>
<tr>
<td>sdee_interval</td>
<td>Default is 600 seconds.</td>
<td></td>
</tr>
<tr>
<td>sdee_port</td>
<td>Default is 443.</td>
<td></td>
</tr>
<tr>
<td>sdee_proxy_port</td>
<td>Default is 8080.</td>
<td></td>
</tr>
<tr>
<td>sdee_use_ssl</td>
<td>Default is T.</td>
<td></td>
</tr>
<tr>
<td>sdee_proxy_ip</td>
<td>Required if use_proxy = T. Default is blank.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3-8  sdee Fields — Start at Column BJ (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>sdee_proxy_username</td>
<td>Required if use_proxy = T. Default is blank.</td>
<td></td>
</tr>
<tr>
<td>sdee_proxy_password</td>
<td>Required if use_proxy = T. Default is blank.</td>
<td></td>
</tr>
<tr>
<td>sdee_use_proxy</td>
<td>Default is F.</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-9  mssql Fields — Start at Column BU

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>mssql_parent</td>
<td>Device type</td>
<td>Default is T. Server = T. Managed device = F</td>
</tr>
<tr>
<td>mssql_port</td>
<td>Used if parent = T. Default is 1433.</td>
<td></td>
</tr>
<tr>
<td>mssql_interval</td>
<td>Used if parent = T. Default is 600 seconds.</td>
<td></td>
</tr>
<tr>
<td>mssql_username</td>
<td>Required if parent = T. Default is blank.</td>
<td></td>
</tr>
<tr>
<td>mssql_password</td>
<td>Required if parent = T. Default is blank.</td>
<td></td>
</tr>
<tr>
<td>mssql_parent_id</td>
<td>Parent name</td>
<td>Required if parent = F. An error is logged if the parent name cannot find the data source.</td>
</tr>
</tbody>
</table>

Table 3-10  syslog Fields — Start at Column CA

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslog_untrust_iface</td>
<td>Most untrusted interface</td>
<td>Required if Vendor is CyberGuard.</td>
</tr>
<tr>
<td>syslog_burb</td>
<td>Internet burb name</td>
<td>Required if Vendor is McAfee and Model is McAfee Firewall Enterprise.</td>
</tr>
<tr>
<td>syslog_sg_mc</td>
<td>Management center flag</td>
<td>Optional if Vendor is Stonesoft Corporation, default is no</td>
</tr>
<tr>
<td>syslog_nsm</td>
<td>Security manager flag</td>
<td>Optional if Vendor is Juniper Networks and Model is Netscreen Firewall/Security Manager or Netscreen IDP, default is no</td>
</tr>
<tr>
<td>syslog_wmi_syslog_format</td>
<td>Optional if Vendor is Microsoft and Model is Adiscon Windows Events, default is 0</td>
<td></td>
</tr>
<tr>
<td>syslog_wmi_version</td>
<td>Optional if Vendor is Microsoft and Model is Adiscon Windows Events, default is Windows 2000</td>
<td></td>
</tr>
<tr>
<td>syslog_aruba_version</td>
<td>Optional if Vendor is Aruba, default is 332</td>
<td></td>
</tr>
<tr>
<td>syslog_rev_pix_dir</td>
<td>Invert network values</td>
<td>Optional if Vendor is Cisco and Model is PIX/ASA or Firewall Services Module, default is no</td>
</tr>
<tr>
<td>syslog_aggregate</td>
<td>Syslog relay</td>
<td>Valid values are blank and Vendor. Default is blank.</td>
</tr>
<tr>
<td>syslog_require_tls</td>
<td>T/F</td>
<td>Indicates if TLS is being used for this data source.</td>
</tr>
<tr>
<td>syslog_syslog_tls_port</td>
<td>The port to be used for syslog TLS if it is being used.</td>
<td></td>
</tr>
<tr>
<td>syslog_mask</td>
<td>Mask for IP address</td>
<td>(Optional) Enables you to apply a mask to an IP address so that a range of IP addresses can be accepted. A zero (0) in the field means that no mask is used. Default is 0.</td>
</tr>
</tbody>
</table>
### Table 3-11 nfxsql Fields — Start at Column CM

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfxsql_port</td>
<td>Default</td>
<td>Default depends on vendor and model:</td>
</tr>
<tr>
<td></td>
<td>Vendor</td>
<td>Model</td>
</tr>
<tr>
<td>Default</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Vendor</td>
<td>Model</td>
<td></td>
</tr>
<tr>
<td>Enterasys</td>
<td>Dragon Sensor or Dragon Squire</td>
<td>9117 Enterasys Networks</td>
</tr>
<tr>
<td>IBM</td>
<td>ISS Real Secure Desktop Protector or ISS Real Secure Network or ISS Real Secure Server Sensor</td>
<td>1433 IBM</td>
</tr>
<tr>
<td>McAfee</td>
<td>ePolicy Orchestrator or ePolicy Orchestrator firewall or ePolicy Orchestrator host IPS</td>
<td>1433 McAfee</td>
</tr>
<tr>
<td>Symantec</td>
<td>Symantec Mail Security for SMTP</td>
<td>3306 Symantec</td>
</tr>
<tr>
<td>Websense</td>
<td>Websense Enterprise</td>
<td>1433 Websense</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Operations Manager</td>
<td>1433 Microsoft</td>
</tr>
<tr>
<td>NetIQ</td>
<td>NetIQ Security Manager</td>
<td>1433 NetIQ</td>
</tr>
<tr>
<td>Trend Micro</td>
<td>Control Manager</td>
<td>1433 Trend Micro</td>
</tr>
<tr>
<td>Zone Labs</td>
<td>Integrity Server</td>
<td>1433 Zone Labs</td>
</tr>
<tr>
<td>Cisco</td>
<td>Security Agent</td>
<td>1433 Cisco</td>
</tr>
<tr>
<td>Sophos</td>
<td>Sophos Antivirus</td>
<td>1127 Sophos</td>
</tr>
<tr>
<td>Symantec</td>
<td>Symantec Antivirus Corporate Edition Server</td>
<td>1433 Symantec</td>
</tr>
<tr>
<td></td>
<td>all others</td>
<td></td>
</tr>
</tbody>
</table>

| nfxsql_userid | Required     |
| nfxsql_password | Required     |

| nfxsql_dbname | Database name | (Optional) Default is blank. |
| nfxsql_splevel | Service Pack level | Used if Vendor is IBM and Model is ISS Real Secure Desktop Protector or ISS Real Secure Network or ISS Real Secure Server Sensor. Default is SP4. |
| nfxsql_version | (Optional) | • Default is 9i if Vendor is Oracle and Model is Oracle Audits.  
• Default is 3.6 if Vendor is McAfee and Model is ePolicy Orchestrator or ePolicy Orchestrator Firewall or ePolicy Orchestrator Host IPS. |

| nfxsql_logtype | Logging type | Required if Vendor is Oracle and Model is Oracle Audits (FGA, GA, or both). |
| nfxsql_sid | Database SID | Optional if Vendor is Oracle and Model is Oracle Audits. Default is blank. |

### Table 3-12 nfxhttp Fields — Start at Column CU

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfxhttp_port</td>
<td>Default is 433.</td>
<td></td>
</tr>
<tr>
<td>nfxhttp_userid</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>nfxhttp_password</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>nfxhttp_mode</td>
<td>Default is secure.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-13  email Fields — Start at Column CY

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>email_port</td>
<td></td>
<td>Default is 993.</td>
</tr>
<tr>
<td>email_mailbox</td>
<td>Mail protocol</td>
<td>Default is imap pop3.</td>
</tr>
<tr>
<td>email_connection</td>
<td>Connection type</td>
<td>Default is ssl pop3.</td>
</tr>
<tr>
<td>email_interval</td>
<td></td>
<td>Default is 600 seconds.</td>
</tr>
<tr>
<td>email_userid</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>email_password</td>
<td></td>
<td>Required</td>
</tr>
</tbody>
</table>

### Table 3-14  estream Fields — Start at Column DE

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>jestream_port</td>
<td></td>
<td>Default is 993.</td>
</tr>
<tr>
<td>jestream_password</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>jestream_estreamer_cert_file</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>jestream_collect_rna</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*These fields are in the spreadsheet. However, a certification file is required, so they are currently ignored.*

### Table 3-15  file source Fields — Start at Column DI

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs_record_lines</td>
<td>Number of lines per record</td>
<td>Used if flat file support. Default is 1.</td>
</tr>
<tr>
<td>fs_file_check</td>
<td>Interval</td>
<td>Default is 15 minutes.</td>
</tr>
<tr>
<td>fs_file_completion</td>
<td></td>
<td>Default is 60 seconds.</td>
</tr>
<tr>
<td>fs_share_path</td>
<td></td>
<td>Default is blank.</td>
</tr>
<tr>
<td>fs_filename</td>
<td>Wildcard expression</td>
<td>Required</td>
</tr>
<tr>
<td>fs_share_name</td>
<td></td>
<td>Required if Protocol is cifs or nfs (not used otherwise).</td>
</tr>
<tr>
<td>fs_username</td>
<td></td>
<td>Used if Protocol is cifs, ftp, or scp. Default is blank.</td>
</tr>
<tr>
<td>fs_password</td>
<td></td>
<td>Used if Protocol is cifs, ftp, or scp. Default is blank.</td>
</tr>
<tr>
<td>fs_encryption</td>
<td></td>
<td>Used if Protocol is ftp or http. Default is no. Also used if flat file support and Protocol are ftp.</td>
</tr>
<tr>
<td>fs_port</td>
<td></td>
<td>Used if Protocol is ftp, default is 990. If Protocol is http, default is 443. Also used if flat file support and Protocol are ftp. Default is 80.</td>
</tr>
<tr>
<td>fs_verify_cert</td>
<td>Verify SSL certificate</td>
<td>Used if Protocol is ftp or http. Default is no. Also used if flat file support and Protocol are ftp.</td>
</tr>
<tr>
<td>fs_compression</td>
<td></td>
<td>Used if Protocol is scp or sftp. Default is no.</td>
</tr>
<tr>
<td>fs_login_timeout</td>
<td></td>
<td>Used if Protocol is scp. Default is 1 second.</td>
</tr>
<tr>
<td>fs_copy_timeout</td>
<td></td>
<td>Used if Protocol is scp. Default is 1 second.</td>
</tr>
<tr>
<td>fs_wmi_version</td>
<td></td>
<td>Used if flat file support and Vendor are Microsoft and Model is Adiscon Windows Events. Default is Windows 2000.</td>
</tr>
<tr>
<td>fs_aruba_version</td>
<td></td>
<td>Used if flat file support and Vendor are Aruba. Default is 332.</td>
</tr>
</tbody>
</table>
**Table 3-15 file source Fields — Start at Column DI** (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs_rev_pix_dir</td>
<td>Invert network values</td>
<td>Used if flat file support and Vendor are Cisco and Model is PIX/ASA or Firewall Services Module. Default is no.</td>
</tr>
<tr>
<td>fs_untrust_iface</td>
<td>Most untrusted interface</td>
<td>Required if flat file support and Vendor are CyberGuard.</td>
</tr>
<tr>
<td>fs_burb</td>
<td>Internet burb name</td>
<td>Required if flat file support and Vendor are McAfee and Model are McAfee Firewall Enterprise.</td>
</tr>
<tr>
<td>fs_nsm</td>
<td>Security manager flag</td>
<td>Optional if flat file support and Vendor are Juniper Networks and Model are Netscreen Firewall/Security Manager or Netscreen IDP. Default is no.</td>
</tr>
<tr>
<td>fs_autolearn</td>
<td>Support generic syslog</td>
<td>Optional if flat file support and Retrieval are gsyslog. Valid values: T, F, COUNT. Default is F.</td>
</tr>
<tr>
<td>fs_type</td>
<td>Generic rule assignment</td>
<td>Required if autolearn = T; otherwise optional. Default is 49190.</td>
</tr>
<tr>
<td>fs_binary</td>
<td></td>
<td>Default is no.</td>
</tr>
<tr>
<td>fs_protocol</td>
<td></td>
<td>Default is ' — Used if parser is Default and collector is nfs File Source.</td>
</tr>
<tr>
<td>fs_delete_files</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 3-16 sql_ms Fields — Start at Column EH**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_ms_port</td>
<td></td>
<td>Default is 1433.</td>
</tr>
<tr>
<td>sql_ms_userid</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>sql_ms_password</td>
<td></td>
<td>Required</td>
</tr>
<tr>
<td>sql_ms_dbname</td>
<td></td>
<td>Database name</td>
</tr>
</tbody>
</table>

**Table 3-17 nas Field — Column EL**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>nas_type</td>
<td></td>
<td>Default is 49190 (User Defined 1). This field is only used for McAfee/PluginProtocol data sources.</td>
</tr>
</tbody>
</table>

**Table 3-18 ipfix Field — Column EM**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipfix_transport</td>
<td></td>
<td>Required. Valid values are TCP and UDP. TCP is the default.</td>
</tr>
</tbody>
</table>

**Table 3-19 snmp Fields — Start at Column EN**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp_authpass</td>
<td>Authentication password</td>
<td>Required if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• tratype = v3trap and secLevel = authPriv or authNoPriv.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• tratype = v3inform and secLevel = authPriv or authNoPriv.</td>
</tr>
<tr>
<td>snmp_authproto</td>
<td>Authentication protocol</td>
<td>Valid values are MD5 or SHA1. Required if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• tratype = v3trap and secLevel = authPriv or authNoPriv.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• tratype = v3inform and secLevel = authPriv or authNoPriv other traptypes. Default is MD5.</td>
</tr>
<tr>
<td>snmp_community</td>
<td>Community name</td>
<td>Required if tratype = v1trap, v2trap, v2inform.</td>
</tr>
<tr>
<td>snmp_engineid</td>
<td></td>
<td>Required if tratype = v3trap</td>
</tr>
</tbody>
</table>
Table 3-19  snmp Fields — Start at Column EN (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp_privpass</td>
<td>Privacy password</td>
<td>Required if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• traptype = snmpv3trap and secLevel = authPriv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• traptype = snmpv3inform and secLevel = authPriv</td>
</tr>
<tr>
<td>snmp_privproto</td>
<td>Privacy protocol</td>
<td>Valid values are: DES and AES. Required if:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• traptype = snmpv3trap and secLevel = authPriv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• traptype = snmpv3inform and secLevel = authPriv</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other traptypes, default is DES.</td>
</tr>
<tr>
<td>snmp_secelevel</td>
<td>Security level</td>
<td>Valid values are: noAuthNoPriv, authNoPriv, and authPriv. Required if</td>
</tr>
<tr>
<td></td>
<td></td>
<td>traptype = v3trap or v3inform.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other traptypes, default is noAuthNoPriv.</td>
</tr>
<tr>
<td>snmp_traptype</td>
<td></td>
<td>Required. Valid values are: v1trap, v2trap, v2inform, v3trap, and v3inform.</td>
</tr>
<tr>
<td>snmp_username</td>
<td></td>
<td>Required if traptype = snmpv3 or snmpv3inform.</td>
</tr>
<tr>
<td>type</td>
<td>Default rule</td>
<td>Required. Default is 49190.</td>
</tr>
<tr>
<td></td>
<td>assignment</td>
<td></td>
</tr>
<tr>
<td>snmp_version</td>
<td></td>
<td>Populated automatically.</td>
</tr>
</tbody>
</table>

Table 3-20  sql_ws — Start at Column EY

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_ws_port</td>
<td></td>
<td>(Optional) Default depends on the vendor. Default for Websense is 1433.</td>
</tr>
<tr>
<td>sql_ws_userid</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>sql_ws_password</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>sql_ws_dbname</td>
<td>(Optional) Default is blank.</td>
<td></td>
</tr>
<tr>
<td>sql_ws_db_instance</td>
<td>Database instance name</td>
<td>Required</td>
</tr>
</tbody>
</table>

Table 3-21  sql — Start at Column FD

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>sql_port</td>
<td>Port used to connect to database</td>
<td></td>
</tr>
<tr>
<td>sql_userid</td>
<td>Database user ID</td>
<td></td>
</tr>
<tr>
<td>sql_password</td>
<td>Database password</td>
<td></td>
</tr>
<tr>
<td>sql_dbinstance</td>
<td>Name of database instance</td>
<td>Valid values are 0 (for the SQL Server Express Database) and 1 (for the SQL Database)</td>
</tr>
<tr>
<td>sql_config_logging</td>
<td></td>
<td>If the value for sql_config_logging is 1, this is gsql.</td>
</tr>
<tr>
<td>sql_protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sql_dbname</td>
<td>Database name</td>
<td></td>
</tr>
</tbody>
</table>

Table 3-22  oracleidm — Start at Column FK

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracleidm_port</td>
<td>Port used to connect to the Oracle Identify Manager database</td>
<td></td>
</tr>
<tr>
<td>oracleidm_userid</td>
<td>User ID for the Oracle Identify Manager database</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-22 oracleidm — Start at Column FK (continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>oracleidm_password</td>
<td>Password for the Oracle Identify Manager database</td>
<td></td>
</tr>
<tr>
<td>oracleidm_ip_address</td>
<td>IP address for the Oracle Identify Manager database</td>
<td></td>
</tr>
<tr>
<td>oracleidm_dpsid</td>
<td>TNS name of the connection being used</td>
<td></td>
</tr>
</tbody>
</table>

### Table 3-23 text — Start at Column FP

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>text_dbinstance</td>
<td>Database instance in which the ePolicy Orchestrator database is running</td>
<td>Fields used for ePolicy Orchestrator data source.</td>
</tr>
<tr>
<td>text_dbname</td>
<td>Name of the ePolicy Orchestrator database</td>
<td></td>
</tr>
<tr>
<td>text_password</td>
<td>Password for the ePolicy Orchestrator database</td>
<td></td>
</tr>
<tr>
<td>text_port</td>
<td>Port used to connect to the ePolicy Orchestrator database</td>
<td></td>
</tr>
<tr>
<td>text_userid</td>
<td>User ID for the ePolicy Orchestrator database</td>
<td></td>
</tr>
</tbody>
</table>

### Table 3-24 gsql — Start at Column FU

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>gsql_port</td>
<td>(Optional) Default depends on the vendor. Default for Websense is 1433.</td>
<td></td>
</tr>
<tr>
<td>gsql_userid</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>gsql_password</td>
<td>Required</td>
<td></td>
</tr>
<tr>
<td>gsql_dbname</td>
<td>(Optional) Default is blank.</td>
<td></td>
</tr>
<tr>
<td>gsql_db_instance</td>
<td>Database instance name Required</td>
<td></td>
</tr>
<tr>
<td>gsql_nsmversion</td>
<td>NSM version Required. If it is left blank, it defaults to version 6.x.</td>
<td></td>
</tr>
</tbody>
</table>

**Migrate data sources to another Receiver**

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **Receiver Properties** for the Receiver with the data sources, then click **Data Sources**.

2. Select the data sources to be migrated, then click **Migrate**.

3. Select the new Receiver in the **Destination Receiver** field, then click **OK**.

**Move data sources to another system**

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

**Before you begin**

To perform this function, you must have device management rights on both Receivers.
Use this process to move data sources from a Receiver located in a secured location to a Receiver in an unsecured location.

There are limitations when exporting data source information:

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

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the data</td>
<td>1 On the system navigation tree, select <strong>Receiver Properties</strong>, then click <strong>Data Source</strong>.</td>
</tr>
<tr>
<td>sources and remote</td>
<td>2 Select the data source, then click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>location</td>
<td>3 Click <strong>Advanced</strong>, then select <strong>Export in NitroFile</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>The data is exported to a remote location and is configured using profile.</strong></td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>From now on, the raw data generated by this data source is copied to the remote share location.</td>
</tr>
<tr>
<td>Create raw data</td>
<td>1 Access the remote share location where the raw data is saved.</td>
</tr>
<tr>
<td>file</td>
<td>2 Save the raw data that has been generated in a location that allows you to move the file to the second Receiver (such as a jump drive that you can carry to the unsecured location).</td>
</tr>
<tr>
<td>Create a file that</td>
<td>1 On the system navigation tree, select <strong>Receiver Properties</strong>, then click **Data Source</td>
</tr>
<tr>
<td>describes the data</td>
<td>2 Locate the file of data sources you moved and click <strong>Upload</strong>.</td>
</tr>
<tr>
<td>sources</td>
<td>3 On the <strong>Remote share profile</strong> list, select the location where you saved the raw data files. If the profile isn't listed, click <strong>Remote share profile</strong> and add the profile.</td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>The data sources are added to the second Receiver and will access the raw data through the remote share profile.</td>
</tr>
<tr>
<td>Import raw data</td>
<td>1 On the system navigation tree, access <strong>Data Sources</strong> on the second Receiver, then click <strong>Import</strong>.</td>
</tr>
<tr>
<td>and data source</td>
<td>2 Locate the file of data sources you moved and click <strong>Upload</strong>. The <strong>Import Data Sources</strong> page lists the data sources to be imported.</td>
</tr>
<tr>
<td>files</td>
<td>3 On the <strong>Remote share profile</strong> list, select the location where you saved the raw data files. If the profile is not listed, click <strong>Remote share profile</strong> and add the profile (see <strong>Configure profiles</strong>).</td>
</tr>
<tr>
<td></td>
<td>4 Click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>

**Set up data source auto-learning**
Set up the ESM to learn IP addresses automatically.

**Before you begin**
Make sure that ports are defined for Syslog, MEF, and flows (see **Set up the interfaces**).
The firewall on the Receiver opens for the time you designate, so the system can learn a set of unknown IP addresses. You can then add to the system as data sources.

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **Receiver Properties**, then click **Data Sources | Auto Learn**.

2. Define the settings as needed, then click **Close**.

**View files generated by data sources**

To view files generated by data sources, you must access the **View Files** page. They can’t be seen on an ESM view.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the McAfee data source.

2. On the actions toolbar, click the **View Files** icon.

3. Do one of the following:
   - Type a file name in the **File name filter** field to locate a specific file.
   - Change the settings in the **Time Range** field to display only the files generated during that time.
   - Click **Refresh** to update the list of files.
   - Select a file on the list, then click **Download** to download the file.

4. Click **Cancel** to close the page.

**User-defined data source types**

This table lists the user-defined types and their corresponding name or entry, which is displayed in the data source editor.

<table>
<thead>
<tr>
<th>ID</th>
<th>Device Model</th>
<th>Vendor</th>
<th>Protocol</th>
<th>Rule Name Prefix</th>
<th>Rule Editor Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>49190</td>
<td>User Defined 1</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined1_</td>
<td>Generic</td>
</tr>
<tr>
<td>49191</td>
<td>User Defined 2</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined2_</td>
<td>Generic</td>
</tr>
<tr>
<td>49192</td>
<td>User Defined 3</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined3_</td>
<td>Generic</td>
</tr>
<tr>
<td>49193</td>
<td>User Defined 4</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined4_</td>
<td>Generic</td>
</tr>
<tr>
<td>49194</td>
<td>User Defined 5</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined5_</td>
<td>Generic</td>
</tr>
<tr>
<td>49195</td>
<td>User Defined 6</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined6_</td>
<td>Generic</td>
</tr>
<tr>
<td>49196</td>
<td>User Defined 7</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined7_</td>
<td>Generic</td>
</tr>
<tr>
<td>49197</td>
<td>User Defined 8</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined8_</td>
<td>Generic</td>
</tr>
<tr>
<td>49198</td>
<td>User Defined 9</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined9_</td>
<td>Generic</td>
</tr>
<tr>
<td>49199</td>
<td>User Defined 10</td>
<td>N/A</td>
<td>syslog</td>
<td>UserDefined10_</td>
<td>Generic</td>
</tr>
</tbody>
</table>
**Supported data sources**

McAfee adds support for new data sources on a regular bases. Receivers can have a maximum of 2000, 200, or 50 data sources on them.

To view a list of data sources that are currently supported, see https://kc.mcafee.com/corporate/index?page=content&id=PD25060

These devices can have 2,000 data sources associated with them:

- ERC-1225
- ERC-1250
- ERC-2230
- ERC-2250
- ERC-2600
- ERC-3450
- ERC-4245
- ERC-4600
- ENMELM-2250
- ENMELM-4245
- ENMELM-4600
- ENMELM-5205
- ENMELM-5600
- ENMELM-5750
- ENMELM-6000
- ELMERC-2230
- ELMERC-2250
- ELMERC-2600
- ELMERC-4245
- ELMERC-4600
- ESMREC-2250
- ESMREC-4245
- ESMREC-5205
- ESMREC-5510

ERC-110 allows only 50 data sources and all others can have a maximum of 200.

These are the maps of the data source ranges:

- Data source types: 1–48,999
- User-defined types: 49,001–49,999
- McAfee reserved (for example, rule sets): 50,001–65,534

⚠️ If you are using a McAfee Firewall Enterprise Event Reporter (ERU), only McAfee data sources are available.

**Configuration for specific data sources**

Some data sources require more information and special configuration settings.

See these sections in this appendix for details.

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

**WMI event log**

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

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

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

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

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

These additional devices are supported from the WMI data source:

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

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

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

**Set up to pull Windows security logs**

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

**Task**

For option definitions, click ? in the interface.

1. Create a new user on the Windows 2008 or 2008 R2 system where you want to read event logs.
2. Assign the user to the Event Log Readers group on the Windows system.
3. Create a new Microsoft WMI Event Log data source on the McAfee Event Receiver, entering the credentials for the user created in Step 1 (see Add a data source).
4. Select Use RPC box, then click OK.
Correlation data source
A correlation data source analyzes data flowing from an ESM, detects suspicious patterns within the data flow, generates correlation alerts that represent these patterns, and inserts these alerts into the Receiver's alert database.

A suspicious pattern is represented by data interpreted by correlation policy rules, which you can create and modify. These types of rules are separate and distinct from Nitro IPS or firewall rules and have attributes that specify their behavior.

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

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

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

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

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

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

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

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

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

```
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+from\s+\{(\S+)\s+port\s+\d+\}?"; raw;
setparm:msg=1; setparm:action=2; setparm:username=5; setparm:src_ip=6; adsid:190; rev:1;)
```

Configuring the ESM
Configuring devices
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 = sdop
- 5 = alert
- 6 = default
- 7 = error
- 8 = success
- 9 = failure
- 10 = emergency
- 11 = critical
- 12 = warning
- 13 = informational
- 14 = debug
- 15 = health
- 16 = add
- 17 = modify
- 18 = remove
- 19 = start
- 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
- 32 = continue
- 33 = infected
- 34 = move
- 35 = move-fail
- 36 = quarantine
- 37 = quarantine-fail
- 38 = remove-fail
- 39 = denied

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

Here is a breakdown of the structure for a rule.

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

**Advanced syslog parser**

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

The ASP can be utilized for syslog devices that are not specifically identified in the Add Data Source page or when the Source Specific Parser doesn’t correctly interpret messages or fully interpret data points related to received events. It is also ideal for sorting through complex log sources such as Linux and UNIX servers. This functionality requires you to write rules (see Add Rules to the Advanced Syslog Parser) tailored to your Linux or UNIX environment.
You can add an ASP data source to the Receiver by selecting Syslog as the vendor (see Add a Data Source). Once you have done this, follow the device manufacturer’s directions to configure your syslog device to send syslog data to the Receiver's IP address.

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

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

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

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

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

Rules are defined as follows.

<table>
<thead>
<tr>
<th>Section</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Header</td>
<td></td>
<td>The rule header contains the Alert action and the any any any format. The rule is: ALERT any any any -&gt; any any</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td>What to do with the event when a match occurs. Options are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ALERT — Log the event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DROP — Log the event but don't forward</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SDROP — Don't log the event or forward</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PASS — Forward if defined, but don't log</td>
</tr>
<tr>
<td>Protocol</td>
<td></td>
<td>If the event defines a protocol, then filter the effective match based on the protocol.</td>
</tr>
<tr>
<td>Src/Dst IP</td>
<td></td>
<td>If the event defines a source or destination IP address, then filter the effective match based on that address.</td>
</tr>
<tr>
<td>Src/Dst Port</td>
<td></td>
<td>If the event defines a source or destination port, then filter the effective match based on that port.</td>
</tr>
<tr>
<td>Rule Body</td>
<td>msg</td>
<td>(Required) The message to associate with this rule. This is the string displayed in the ESM Thin Client for reporting purposes unless overridden with a pcre/setparm detected message (see below). The first work of the msg is the category name followed by actual message (msg: &quot;category rule message&quot;).</td>
</tr>
<tr>
<td></td>
<td>content</td>
<td>(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: &quot;search 1&quot;; content &quot;something else&quot;)</td>
</tr>
<tr>
<td><strong>Section</strong></td>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td>procname</td>
<td>On many UNIX and Linux systems, the process name (and process ID) is part of a standardized syslog message header. The procname keyword can be used to filter Event matches for the Rule. Used to exclude or filter Event matches where two processes on a Linux or UNIX server may have similar or the same message text.</td>
</tr>
<tr>
<td></td>
<td>adsid</td>
<td>The data source ID to use. This value overrides the Default Rule Assignment in the data source editor.</td>
</tr>
<tr>
<td></td>
<td>sid</td>
<td>Signature ID of the Rule. This is the match ID used in the ESM Thin Client unless overridden with a pcre/setparm detected sid.</td>
</tr>
<tr>
<td></td>
<td>rev</td>
<td>Rule revision. Used to track changes.</td>
</tr>
<tr>
<td></td>
<td>severity</td>
<td>Value between 1 (least severe) and 100 (most severe) assigned to events matching the rule.</td>
</tr>
<tr>
<td></td>
<td>pcre</td>
<td>The PCRE keyword is a Perl Compatible Regular Expression match against incoming events. The PCRE is quote delimited and all occurrences of &quot;/&quot; is treated as a normal character. Content in parentheses is held for the use of the setparm keyword. The PCRE keyword can be modified by nocase, nomatch, raw and setparm keywords.</td>
</tr>
<tr>
<td></td>
<td>nocase</td>
<td>Causes the PCRE content to be matched whether the case matches or not.</td>
</tr>
<tr>
<td></td>
<td>nomatch</td>
<td>Inverts the PCRE match (equivalent to !~ in Perl).</td>
</tr>
<tr>
<td></td>
<td>raw</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>setparm</td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Tag</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>* sid</td>
<td>This captured parameter overrides the matched rule’s sid.</td>
</tr>
<tr>
<td>* msg</td>
<td>This captured parameter overrides the matched rule’s message or name.</td>
</tr>
<tr>
<td>* action</td>
<td>This captured parameter indicates what action the third-party device took.</td>
</tr>
<tr>
<td>* protocol</td>
<td></td>
</tr>
<tr>
<td>* src_ip</td>
<td>This replaces the syslog source’s IP which is the default source IP of an event.</td>
</tr>
<tr>
<td>* src_port</td>
<td></td>
</tr>
<tr>
<td>* dst_ip</td>
<td></td>
</tr>
<tr>
<td>* dst_port</td>
<td></td>
</tr>
<tr>
<td>* src_mac</td>
<td></td>
</tr>
<tr>
<td>* dst_mac</td>
<td></td>
</tr>
<tr>
<td>* genid</td>
<td>This is used to modify the sid as stored in the database, used for non-McAfee snort matches in snort preprocessors.</td>
</tr>
<tr>
<td>* url</td>
<td>Reserved, but not used yet.</td>
</tr>
<tr>
<td>* src_username</td>
<td>First/source user name.</td>
</tr>
<tr>
<td>* username</td>
<td>Alternate name for src_username.</td>
</tr>
<tr>
<td>* dst_username</td>
<td>Second/destination user name.</td>
</tr>
<tr>
<td>Tag</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>* domain</td>
<td>Must be an integer.</td>
</tr>
<tr>
<td>* hostname</td>
<td></td>
</tr>
<tr>
<td>* application</td>
<td></td>
</tr>
<tr>
<td>* severity</td>
<td></td>
</tr>
<tr>
<td>* action map</td>
<td>Allows you to map specific actions of your product to the McAfee actions.</td>
</tr>
<tr>
<td></td>
<td>The action map is case sensitive. Example: alert any any any -&gt; any any</td>
</tr>
<tr>
<td></td>
<td>(msg:&quot;OpenSSH Accepted Password&quot;; content:&quot;Accepted password for &quot;;</td>
</tr>
</tbody>
</table>
|             | action_map:Accepted=8, Blocked=3; pcre:"(Accepted)\s+password\s+for\s+(\S+
<p>|             | +)\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 -&gt; any any (msg:&quot;OpenSSH Accepted Password&quot;; content:&quot;Accepted password for &quot;; severity_map:High=99, Low=25, 10=99, 1=25; pcre:&quot;(Accepted)\s+password\s+for\s+(\S+)\s+from\s+(d+\|d+|d+|d+)\s+port\s+(d+)&quot;; setparm:action=1; sid:31; rev:1;)). See Severity and Action Map for details. |
| * var       | This is another way to use setparms. The beneficial use, however, is the use of |
|             | creating one value from multiple captures of multiple PCREs. You can create more |
|             | than one PCRE that captures only a small portion of your string rather than one |
|             | large PCRE with multiple captures. Here's an example of capturing a user name, |
|             | domain, and creating an email address to store in the objectname field.       |
|             | • Syntax = var:field=${PCRE:Capture}                                         |
|             | • PCRE = not the actual PCRE but the number of the pcre. If your rule has two |
|             | PCRE's you would have a PCRE of 1 or 2.                                      |
|             | • Capture = not the actual capture but the number (first, second or third capture |
|             | [1,2,3])                                                                     |
|             | • Sample Message: A man named Jim works for McAfee.                         |
|             | • PCRE: (Jim).*?(McAfee)                                                    |
|             | • Rule: alert any any any -&gt; any any (msg:&quot;Var User Jim&quot;; content:&quot;Jim&quot;;   |
|             | pcre:&quot;(Jim)&quot;; pcre:&quot;(McAfee)&quot;; var:src_username=${1:1}; var:domain=${2:1};  |
|             | var:objectname=${1:1}@${2:1}.com raw; classtype:unknown; adsid:190; sev:25;  |
|             | sid:610061000; rev:1; normID:1209008128; gensys:T;)                          |
|             | • Mapped Source User: Jim                                                  |
|             | • Mapped Domain: McAfee                                                    |
|             | • Mapped objectname: <a href="mailto:Jim@McAfee.com">Jim@McAfee.com</a>                                        |
| * sessionid | This is an integer.                                                         |
| * commandname | This is a string value.                                                   |
| * objectname | This is a string value.                                                    |
| * event_action | This tag is used to set a default action. You can’t use event_action and action_map in the same rule. For example, if you had an event for a Successful Login you could use the event_action tag and default the action to success (for example, event_action:8;). |</p>
<table>
<thead>
<tr>
<th>Tag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>* firsttime_fmt</td>
<td>Used to set the first time of the event. See list of formats.</td>
</tr>
<tr>
<td>* lasttime_fmt</td>
<td>Used to set the last time of the event. You can use this with a setparm or a</td>
</tr>
<tr>
<td></td>
<td>var (var:firsttime=&quot;${1:1}&quot; or setparm:lasttime=&quot;1&quot;). For example:</td>
</tr>
<tr>
<td></td>
<td>alert any any any -&gt; any any (msg:&quot;SSH Login Attempt&quot;; content:&quot;content&quot;;</td>
</tr>
<tr>
<td></td>
<td>firsttime_fmt: &quot;%Y-%m-%dT%H:%M:%S.%f&quot;; lasttime_fmt: &quot;%Y-%m-%dT%H:%M:%S.%f&quot;</td>
</tr>
<tr>
<td></td>
<td>pcre:&quot;PCRE goes here; raw; setparm:firsttime=1;</td>
</tr>
<tr>
<td></td>
<td>setparm:lasttime=1; adsid:190; rev:1;)</td>
</tr>
<tr>
<td></td>
<td>For current formats supported, see <a href="http://pubs.opengroup.org/onlinepubs/">http://pubs.opengroup.org/onlinepubs/</a></td>
</tr>
<tr>
<td></td>
<td>009695399/functions/strptime.html for more detail.</td>
</tr>
<tr>
<td></td>
<td>%Y - %d - %m %H : %M : %S</td>
</tr>
<tr>
<td></td>
<td>%m - %d - %Y %H : %M : %S</td>
</tr>
<tr>
<td></td>
<td>%b %d %Y %H : %M : %S</td>
</tr>
<tr>
<td></td>
<td>%b %d %Y %H - %M - %S</td>
</tr>
<tr>
<td></td>
<td>%b %d %H : %M : %S %Y</td>
</tr>
<tr>
<td></td>
<td>%b %d %H - %M - %S %Y</td>
</tr>
<tr>
<td></td>
<td>%b %d %H : %M : %S</td>
</tr>
<tr>
<td></td>
<td>%b %d %H - %M - %S</td>
</tr>
<tr>
<td></td>
<td>%Y %H : %M : %S</td>
</tr>
<tr>
<td></td>
<td>%Y %H - %M - %S</td>
</tr>
<tr>
<td></td>
<td>%m - %d - %Y</td>
</tr>
<tr>
<td></td>
<td>%H : %M : %S</td>
</tr>
<tr>
<td></td>
<td>%H - %M - %S</td>
</tr>
<tr>
<td></td>
<td>%Y is 4-digit year</td>
</tr>
<tr>
<td></td>
<td>%m is month number (1-12)</td>
</tr>
<tr>
<td></td>
<td>%d is date (1-31)</td>
</tr>
<tr>
<td></td>
<td>%H is hours (1-24)</td>
</tr>
<tr>
<td></td>
<td>%M is minutes (0-60)</td>
</tr>
<tr>
<td></td>
<td>%S is seconds (0-60)</td>
</tr>
<tr>
<td></td>
<td>%b is month abbreviation (jan, feb)</td>
</tr>
</tbody>
</table>

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

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

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

**Add an ASP data source with different encoding**

The ESM reads UTF-8 encoded data. If you have an ASP data source that generates data with different encoding, you must indicate that when adding the data source.
**Task**
For option definitions, click ? in the interface.

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

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

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

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

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

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

The Receiver is able to extract this information from an SDEE/CIDEE event:
- Source and destination IP addresses
- Source and destination ports
- Protocol
- Event time
- Event count (CIDEE provides a form of event aggregation, which the Receiver honors)
- Signature ID and sub-ID
- The ESM event ID is calculated from the SDEE signature ID and the CIDEE sub-signature ID using the following formula:
  \[ \text{ESMI ID} = (\text{SDEE ID} \times 1000) + \text{CIDEE sub-ID} \]
  So, if the SDEE signature ID is 2000 and the CIDEE sub-signature ID is 123, the ESMI event ID would be 2000123.
- VLAN
- Severity
- Event description
- Packet contents (if available).

If the Receiver is connecting to the SDEE provider for the first time, the current date and time is used as a starting point for requesting events. Future connections request all events since the last successful pull.
**Configure ePolicy Orchestrator 4.0**
The McAfee Event Receiver Data Source for ePolicy Orchestrator now supports ePolicy Orchestrator 4.0. ePolicy Orchestrator 4.0 stores events in SQL Server database. The ePolicy Orchestrator data source connects to this SQL server database through JDBC to pull events information. A new user name (ID) and password must be created within the ePolicy Orchestrator database for use in conjunction with the data source for ePolicy Orchestrator.

**Task**
For option definitions, click ? in the interface.

1. Log in to the ePolicy Orchestrator database server.
2. Launch SQL Server Enterprise Manager by selecting Start | All Programs | Microsoft SQL Server | Enterprise Manager.
3. Expand the Console Root node several times to view the items located under the Security folder.
4. Right-click the Logins icon, then select New Login from the menu.
5. On the SQL Server Login Properties-New Login page, fill in the following on the General tab:
   a. In the Name field, enter the user name you want to use for data source for ePolicy Orchestrator to connect to the ePolicy Orchestrator database (for example, nfepo).
   b. In Authentication, select SQL Server Authentication Password, then enter the password.
   c. In Defaults, select the ePolicy Orchestrator database (ePO4_<hostname>) from the Database drop-down list.

   **Tip:** If you leave default Database as master, data source for ePolicy Orchestrator fails to pull events.
6. On the Database Access tab, select Permit associated with the ePolicy Orchestrator database.
7. For Permit in Database Role, select db_datareader, then click OK.
8. Confirm the new password, then click OK.

**Add an ArcSight data source**
Add data sources for an ArcSight device.

**Task**
For option definitions, click ? in the interface.

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

The data received from ArcSight is parsed so it can be viewed on the ESM console.
Common Event Format (CEF)

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

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

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

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

- **Version** is an integer and identifies the version of the CEF format. Event consumers use this information to determine what the fields represent. Currently only version 0 (zero) is established in the above format. Experience might show that other fields must be added to the "prefix" and therefore require a version number change. Adding new formats is handled through the standards body.

- **Device Vendor**, **Device Product**, and **Device Version** are strings that uniquely identify the type of sending device. No two products may use the same device-vendor and device-product pair. There is no central authority managing these pairs. Event producers have to ensure that they assign unique name pairs.

- **DeviceEventClassId** is a unique identifier per event-type. This can be a string or an integer. DeviceEventClassId identifies the type of event reported. In the intrusion detection system (IDS) world, each signature or rule that detects certain activity has a unique deviceEventClassId assigned. This is a requirement for other types of devices as well, and helps correlation engines deal with the events.

- **Name** is a string representing a human-readable and understandable description of the event. The event name should not contain information that is specifically mentioned in other fields. For example: "Port scan from 10.0.0.1 targeting 20.1.1.1" is not a good event name. It must be: "Port scan." The other information is redundant and can be picked up from the other fields.

- **Severity** is an integer and reflects the importance of the event. Only numbers from 0 to 10 are allowed, where 10 indicates the most important event.

- **Extension** is a collection of key-value pairs. The keys are part of a predefined set. The standard allows for including additional keys as outlined later. An event can contain any number of key-value pairs in any order, separated by spaces. If a field contains a space, such as a file name, this is okay and can be logged in exactly that manner. For example:

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

Here is a sample message to illustrate appearance:

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

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

CEF:0|NetWitness|Informer|1.6|{name}|{name}|Medium | externalId={#sessionid}
proto={#ip.proto} categorySignificance=/Normal categoryBehavior=/Authentication/Verify
categoryDeviceGroup=/OS categoryOutcome=/Attempt categoryObject=/Host/Application/
Service act={#action} deviceDirection=0 shost={#ip.host} src={#ip.src}
The correct format requires you to change "dport" above to "dpt."

**Adiscon setup**

Syslog WMI is supported through Adiscon.

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

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

**Syslog relay support**

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

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

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

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

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

The header on the syslog must be configured to look like the following example: 1 <123> 345 Oct 7 12:12:12 2012 mcafee.com httpd[123] where
Run NSM-SIEM configuration tool
Prior to setting up an NSM data source, you must run the NSM-SIEM Configuration Tool.

Task
For option definitions, click ? in the interface.

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

2 Run the configuration tool on the NSM server.
   The tool must find the default path to the NSM. If it does not locate it, browse to it.

3 Enter the NSM SQL user, password, and database name that was entered in the install of NSM.

4 Enter the SIEM user name and password on the data source and Receiver IP address where the data source is added.
   These are entered on the data source screen.

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

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

   Database Name is required. If the database name contains a dash, you must enclose the name in brackets (for example, [ePO4_WIN-123456]).
The **ePO Query** option allows you to query the ePolicy Orchestrator device and create client data sources. If the default **Match by type** is selected in the **Use client data sources** field and you click **ePO Query**, the ePolicy Orchestrator device is queried and any supported ePolicy Orchestrator products are added as client data sources.

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

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

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

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

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

**IBM Internet Security System SiteProtector**

The Receiver is capable of retrieving events from an Internet Security Systems (ISS) SiteProtector server by querying the Microsoft SQL Server database SiteProtector used to store its events. Unlike some of the other types of data sources supported by the Receiver, retrieving events from a SiteProtector server is done using a "pull" model instead of a "push" model. This means that periodically, the Receiver contacts the SiteProtector database and requests any new events since the last event pulled. Each time events are retrieved from the SiteProtector server they are processed and stored in the Receiver’s event database, ready to be retrieved by the ESM.

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

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

The **Advanced** option at the bottom of the page allows you to define a URL that can be used to launch specific URLs when viewing event data. You can also define a vendor, product, and version to be used for Common Event Format (CEF) event forwarding. These settings are optional.
For the Receiver to query the SiteProtector database for events, the Microsoft SQL Server installation hosting the database used by SiteProtector must accept connections from the TCP/IP protocol.

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

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

The Receiver extracts this information from a SiteProtector event:

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

**Set up Check Point**

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

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

**Task**

For option definitions, click ? in the interface.

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

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

2. Click Options.

3. On the Advanced Settings page, select the communication method, then type the Server Entity Distinguished Name of this data source.

4. Click OK twice.

5. Do the following, if needed:
If you receive this error...  
Do the following...

<table>
<thead>
<tr>
<th>SIC Error for lea: Client could not choose an authentication method for service lea</th>
<th>Verify that you selected the correct settings for Use Authentication and Use Encryption when you added the Check Point data source.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you selected Use Authentication only, the OPSEC client attempts to communicate with the log server using &quot;sslca_clear&quot;. If you selected Use Authentication and Use Encryption, the OPSEC client attempts to communicate with the log server using &quot;sslca.&quot; If you selected neither, the OPSEC client attempts to communicate with the log server using &quot;none.&quot;</td>
</tr>
</tbody>
</table>

2 Verify that the OPSEC application you are using to communicate with the Check Point log server has LEA selected in the Client Entities section.

3 If both of these steps verify correctly, locate the sic_policy.conf file on your Check Point Log Server installation. For example, on a Linux-based R65 system, the file is located in /var/opt/CPshrd-R65/conf.

4 When you determine which communication method (authentication method in the file) allows LEA communication method to the Log Server, select that communication method on the Advanced Settings page as Communication Method.

<table>
<thead>
<tr>
<th>SIC Error for lea: Peer sent wrong DN: &lt;expected dn&gt;</th>
<th>• Provide a string for the Server Entity Distinguished Name text box by entering the string that represents &quot;&lt;expected dn&gt;&quot; in the error message.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>An alternative is to find the distinguished name for the Check Point Log Server by looking at the Check Point Log Server's network object in the Smart Dashboard UI.</td>
</tr>
<tr>
<td></td>
<td>The DN of the SMS/CMA will be like that of the DN for the OPSEC app, just replace the first entry with CN=cp_mgmt. For instance consider an OPSEC app DN of CN=mcafee_OPSEC,O=r75..n55nc3. The SMS/CMA DN will be CN=cp_mgmt,O=r75..n55nc3. The DN of the log server would be like this, CN=CPlogserver,O=r75..n55nc3.</td>
</tr>
</tbody>
</table>

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

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

McAfee rulesets

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

<table>
<thead>
<tr>
<th>Data Source ID</th>
<th>Display Name</th>
<th>Corresponding RSID</th>
<th>Rule Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>50201</td>
<td>Firewall</td>
<td>0</td>
<td>2,000,000–2,099,999</td>
</tr>
<tr>
<td>50202</td>
<td>Custom Firewall</td>
<td>0</td>
<td>2,200,000–2,299,999</td>
</tr>
<tr>
<td>50203</td>
<td>Custom Signatures</td>
<td>0</td>
<td>5,000,000–5,999,999</td>
</tr>
<tr>
<td>50204</td>
<td>Internal</td>
<td>0</td>
<td>3,000,000–3,999,999</td>
</tr>
<tr>
<td>50205</td>
<td>Vulnerability and Exploit</td>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td>50206</td>
<td>Adult Content</td>
<td>5</td>
<td>N/A</td>
</tr>
<tr>
<td>50207</td>
<td>Chat</td>
<td>8</td>
<td>N/A</td>
</tr>
<tr>
<td>50208</td>
<td>Policy</td>
<td>11</td>
<td>N/A</td>
</tr>
<tr>
<td>50209</td>
<td>Peer to Peer</td>
<td>14</td>
<td>N/A</td>
</tr>
<tr>
<td>50210</td>
<td>Multimedia</td>
<td>17</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Receiver asset sources

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

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

If two asset discovery sources (such as Vulnerability Assessment and Network Discovery) find the same asset, the discovery method with the highest priority adds the asset it discovered to the table. If two discovery sources have the same priority, the last one that discovers the asset takes priority over the first.

**Add asset source**

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

**Task**

For option definitions, click ? in the interface.

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

### Enterprise Log Manager (ELM) settings

ELM supports the storage and management of, access to, and reporting of log data.

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

The ELM provides the capability to set up search and integrity-check jobs. Each of these jobs accesses the stored logs and retrieves or checks the data that you define in the job. You can then view the results and choose to export the information.
The information provided applies to all these ELM device models:

- ENMELM-5205 (ESM/Log Manager Combo)
- ENMELM-5510 (ESM/Log Manager Combo)
- ENMELM-4245 (ESM/Log Manager Combo)
- ENMELM-4245 (ESM/Log Manager Combo)
- ELM-5205
- ELM-5510
- LMERC 2230 (Receiver/Log Manager Combo)

To configure an ELM, you must know:

- The sources that are storing logs on the ELM
- The storage pools that are required and their data retention times
- The storage devices that are required to store the data

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

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

2. Configure ELM storage devices to meet the estimated requirements.

3. Acquire logs on the ELM for a short period.

4. Use ELM storage statistics information to change the storage device configurations to accommodate the actual data storage requirements.

**Preparing to store data on the ELM**

There are several steps you must take to configure an ELM to store data.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Define data retention times        | Based on ELM installation requirements, define the number of different data retention times needed. These are common data retention times:  
  - SOX – 7 years  
  - PCI – 1 year  
  - GLBA – 6 years  
  - EU DR Directive – 2 years  
  - Basel II – 7 years  
  - HIPAA – 6 or 7 years  
  - NERC – 3 years  
  - FISMA – 3 years  |
<p>| 2    | Define sources of log data         | The goal here is to define all sources of logs that are stored on the ELM and to estimate the average log byte size and average logs generated per day for each. This only needs to be an estimate. It might be easier to estimate the average log byte size and average logs generated per day for types of sources (such as Firewall, router, Nitro IPS, ADM, DEM, ELM), then estimate the number of sources for each type. The next step requires the association of each source with a retention time defined in Step 1, so be sure to take that into consideration when estimating source types (for example, SOX Firewall, PCI DEM). |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Define storage pools</td>
<td>Based on ELM installation requirements, associate each source of logs, or source, with a data retention time, defining the set of storage pools required for the ELM installation.</td>
</tr>
</tbody>
</table>
| 4    | Estimate storage pool size requirements | For each storage pool, estimate its storage requirements using one of the following equations:  
- Using individual sources:  
  \[ \text{IRSGB} = 0.1 \times (\text{DRTD} \times \text{SUM} (\text{DSAB} \times \text{DSALPD})) / (1024 \times 1024 \times 1024) \]  
  Where  
  \( \text{IRSGB} \) = Initial required storage in gigabytes  
  \( \text{DRTD} \) = Data retention time in days  
  \( \text{SUM()} \) = The sum for all data sources  
  \( \text{DSAB} \) = Data source average bytes per log  
  \( \text{DSALPD} \) = Data source average logs per day  
- Using source types:  
  \[ \text{IRSGB} = 0.1 \times (\text{DRTD} \times \text{SUM} (\text{NDS} \times \text{DSTAB} \times \text{DSTALPD})) / (1024 \times 1024 \times 1024) \]  
  Where  
  \( \text{IRSGB} \) = Initial required storage in gigabytes  
  \( \text{DRTD} \) = Data retention time in days  
  \( \text{NDS} \) = Number of data sources of a data source type  
  \( \text{SUM()} \) = The sum for all data source types  
  \( \text{DSTAB} \) = Data source type average bytes per log  
  \( \text{DSTALPD} \) = Data source type average logs per day |
| 5    | Create initial storage devices | Create one or more ELM storage devices so they are large enough to store each IRSGB worth of data (see Add a storage device). |
| 6    | Create storage pools | For each storage pool you defined in Step 3, create an ELM storage pool using the associated retention time from Step 1, the associated IRSGB values from Step 4, and the associated storage devices from Step 5 (see Add a storage pool). |
| 7    | Start logging data | Configure sources to send their logs to the ELM, and let them do so for one or two days. |
| 8    | Refine storage pool size requirement estimates | For each storage pool created in Step 6, refine its storage requirement estimate using the following equation:  
  \[ \text{RSGB} = 1.1 \times \text{DRTD} \times \text{SPABRPD} / (1024 \times 1024 \times 1024) \]  
  Where  
  \( \text{RSGB} \) = Required storage in gigabytes  
  \( \text{DRTD} \) = Data retention time in days  
  \( \text{SPABRPD} \) = Storage pool’s daily “Avg. byte rates” value from its Statistical Report |
| 9    | Modify or create storage devices | For each RSGB value from Step 8, modify or create ELM storage devices so that they are large enough to store RSGB worth of data. |
| 10   | Modify storage pools | If needed, modify each storage pool created in Step 6 by adding storage devices created in Step 9, or increase existing storage device allocation. |
Setting up ELM storage

To store logs, the ELM must have access to one or more storage devices. The storage requirement for an ELM installation is a function of the number of data sources, their logging characteristics, and their data retention time requirements. The storage requirement varies over time because all are likely to change during the life of an ELM installation.

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

ELM storage terminology

Review these terms to work with ELM storage:

- **Storage Device** — A data storage device accessible to an ELM. Some ELM models offer an onboard storage device, some offer a SAN connection capability, and some both. All ELM models offer a NAS connection capability.

- **Storage Allocation** — A specific amount of data storage on a specific storage device (for example, 1TB on a NAS storage device).

- **Data Retention Time** — The amount of time a log is stored.

- **Storage Pool** — One or more storage allocations, which together specify a total amount of storage, coupled with a data retention time that specifies the maximum number of days a log is to be stored.

- **Log Source** — Any source of logs that an ELM stores.

ELM storage device types

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

<table>
<thead>
<tr>
<th>Device type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS</td>
<td>If you need to edit the remote mount point of the storage device containing the ELM Management Database, use the Migrate DB option to move the database to a different storage device (see Migrate ELM database). You can then safely change the remote mount point field and move the database back to the updated storage device.</td>
</tr>
</tbody>
</table>
| CIFS        | • Using the CIFS share type with Samba server versions greater than 3.2 can result in data loss.  
• When connecting to a CIFS share, don't use commas in your password.  
• If you are using a Windows 7 computer as a CIFS share, see Disable HomeGroup file sharing. |
| iSCSI       | • When connecting to an iSCSI share, don't use commas in your password.  
• Attempting to attach multiple devices to one IQN can cause data loss and other configuration problems. |
| SAN         | The SAN option is available only if there is a SAN card installed on the ELM and there are SAN volumes available. |

Disable HomeGroup file sharing

Windows 7 requires you to use HomeGroup file sharing, which works with other Windows 7 computers but not with Samba. To use a Windows 7 computer as a CIFS share, you must disable HomeGroup file sharing.
Task
For option definitions, click ? in the interface.

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

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

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

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Storage Pools.
2. Click Add next to the top table.
3. On the Add Storage Device page, fill in the requested information.
4. Click OK to save the settings.
   The device is added to the list of available ELM storage devices.

You can edit or delete storage devices from the table on the Storage Pools page.
Move a storage pool
You can move a storage pool from one device to another.

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select the ELM device holding the storage pool, then click the Properties icon.

2. Click Storage Pools.

3. In the Storage Pools table, click the mirrored devices listed under the pool to be moved.

4. Click Edit, and from the Data Storage Devices drop-down list, select the device that mirrors the storage pool to be moved.

   It is now the main data storage device.

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

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

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Storage Pool.

2. On the bottom table, select the pool to be reduced, then click Reduce Size.

3. Enter the amount you want to reduce the storage by, then click OK.

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

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

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

A mirrored storage pool might lose connection with its storage device. The loss can be due to:
• The file server or the network between the ELM and the file server has failed.
• The file server or network is shut down for maintenance.
• An allocation file is accidentally deleted.

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

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

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Storage Pools.
2. Click Add next to the bottom table
3. On the Add Storage Pool page, enter the information requested, then click Add to select the storage device and mirroring device.
   
   ![](image)

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

4. Click OK twice.

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Storage Pool.
2. Hover over the mirrored devices that are showing a warning icon.
   
   A tool tip informs you that the ELM allocation is rebuilding or that the mirrored device needs to be rebuilt.

3. To rebuild the mirrored devices, click on the devices, then click Rebuild.
   
   When the process is complete, you are notified that the allocation rebuilt successfully.

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

For option definitions, click ? in the interface.

1. On the system navigation tree, select the ELM currently holding the mirroring storage pool in the system navigation tree, then click the Properties icon.

2. Click Storage Pools, then select the mirrored devices in the Storage Pool table and click Edit.

3. Do one of the following:
   - If the device selected in the Mirrored Data Storage Device field is the one you want to disable, click the drop-down arrow in that field and select a different device to mirror the data storage device or select None.
   - If the device selected in the Data Storage Device field is the one you want to disable, click the drop-down arrow in that field and select a different device to act as the data storage device.

4. Click OK to save the changes.

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

**Set up external data storage**

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Data Storage.

2. Click the iSCSI, SAN, or DAS tab, then follow the required steps.

3. Click Apply or OK.

**Add an iSCSI device**

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Data Storage.

2. On the iSCSI tab, click Add.

3. Enter the information requested, then click OK.

If the connection is successful, the device and its IQNs are added to the iSCSI Configuration list, as well as the Device Type list on the Add Storage Device page (see Add a storage device).

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

4. Prior to using an IQN for ELM storage, select it on the list, then click Format.
5 To check its status as it is formatting, click Check Status.

6 To discover or rediscover the IQNs, click the iSCSI device, then click Discover.

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

**Format a SAN storage device to store ELM data**

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

❗️ Before you begin

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

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, select ELM Properties, then click Data Storage.

2 Click the SAN tab, then check the status of the SAN volumes that were detected.

- **Format required** — The volume must be formatted and doesn't appear on the list of available volumes on the Add Storage Device page.

- **Formatting** — The volume is in the process of being formatted and doesn't appear on the list of available volumes.

- **Ready** — The volume is formatted and has a recognizable file system. These volumes can be used to store ELM data.

3 If a volume is not formatted and you want it to store data, click it, then click Format.

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

4 To check if formatting is complete, click Refresh.

If formatting is completed, the status changes to Ready.

5 To view the details of a volume at the bottom of the page, click the volume.

You can now set up the formatted SAN volume as a storage device for ELM storage.

**Assign a DAS device to store data**

You can assign available DAS devices to store ELM data.

❗️ Before you begin

Set up DAS devices.

**Task**

For option definitions, click ? in the interface.

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

ℹ️ On an all-in-one device, you can assign the DAS to the ESM by selecting the ESM, then clicking the Properties icon.
2 Click Data Storage, then click the DAS tab.

The DAS table lists the devices that are available for storage.

3 On the table, click one of the devices that has not been assigned to store ELM or ESM data.

4 Click Assign, then click Yes on the warning page.

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

The ELM restarts.

**ELM redundancy**

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

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

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

**Switch over**

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

**Return to service**

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

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

**Suspend**

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

**Disable redundancy on the ELM**

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

**View status**

You can view details on the state of data synchronization between the active and standby ELM by selecting Status.
Set up ELM redundancy
If you have a standalone ELM device on your system, you can provide redundancy for logging by adding a standby ELM.

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

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, click the ELM, then click the Properties icon.
2. On the ELM Properties page, click ELM Redundancy, then click Enable.
3. Type the IP address and password for the standby ELM, then click OK.
4. On the ELM Properties page, click Storage Pools, and verify that the Active tab is selected.
5. Add storage devices to the active ELM (see Add a storage device to link to a storage pool).
6. Click the Standby tab, then add storage devices that have enough combined space to match the storage on the active ELM.
7. Add one or more storage pools to each ELM (see Add or edit a storage pool).

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

Managing ELM compression
Compress the data coming in to the ELM to save disk space or process more logs per second. The three options are Low (default), Medium, and High. This table shows details about each level.

<table>
<thead>
<tr>
<th>Level</th>
<th>Compression rate</th>
<th>Percentage of maximum compression</th>
<th>Percentage of maximum logs processed per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>14:1</td>
<td>72%</td>
<td>100%</td>
</tr>
<tr>
<td>Medium</td>
<td>17:1</td>
<td>87%</td>
<td>75%</td>
</tr>
<tr>
<td>High</td>
<td>20:1</td>
<td>100%</td>
<td>50%</td>
</tr>
</tbody>
</table>

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

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

Set ELM compression
Select the compression level for the data coming in to the ELM to save disk space or process more logs.
**Task**
For option definitions, click ? in the interface.

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

You are notified when the level is updated.

**View results of a search or integrity check**
When a search or integrity check job is completed, you can view the results.

**Before you begin**
Run a search or integrity check job that produces results.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **ELM Properties**.
2. Click **Data**, then select the **Search Logs and Files** or **Integrity Check** tab.
3. Highlight the job that you want to view on the **Search Results** table, then click **View**.

The **ELM search results** page displays the results of the job.

- All ELM searches can be lost if you remove more than one extra VM drive from the ESM at one time. To avoid losing the results, export the ELM search results.

**Back up and restore ELM**
If there is a system failure or data loss, you must back up the current settings on ELM devices. All configuration settings, including the ELM logging database, are saved. The actual logs that are stored on the ELM are not backed up.

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

**Task**
For option definitions, click ? in the interface.

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

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up ELM now</td>
<td>Provide the requested information, then click <strong>Backup Now</strong>.</td>
</tr>
<tr>
<td>Back up ELM settings automatically</td>
<td>Select the frequency and provide the information.</td>
</tr>
<tr>
<td>Restore backup now</td>
<td>Click <strong>Restore Backup Now</strong>. The ELM database is restored to the settings from a previous backup.</td>
</tr>
</tbody>
</table>
Restore ELM management database and log data
To replace an ELM, restore the management database and log data to the new ELM. For this to work, the database and log data must be mirrored.

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

**Task**
For option definitions, click ⬤ in the interface.

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

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

Enable faster ELM searches
The full-text indexing engine indexes ELM logs. When it is enabled, it provides faster ELM search speeds because it limits the number of files that must be searched.

**Before you begin**
Define the storage device and space allocated to the indexer. The number of ELM logs that can be indexed vary based on the space you allocate for the indexer.

**Task**
For option definitions, click ⬤ in the interface.

1. On the system navigation tree, select ELM Properties, then click ELM Configuration | Full Text Index.
2. Make the required selections on the Select Full Text Indexer Location page.
3. Click OK to save the settings.

View ELM storage usage
Viewing the usage of storage on the ELM can help you make decisions regarding space allocation on the device.
Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click ELM Management.
2. Click View Usage.

The Usage Statistics page opens, showing the statistics for the storage device and pools on the ELM.
3. Click OK.

Migrating ELM database
The ELM management database stores the records that keep track of the logs sent to the ELM. The amount of disk space that is available on your ELM device to store the management database depends on the model.

When you first add the device, the system verifies if it has enough disk space to store the records. If it doesn't, you are prompted to define an alternate location for management database storage. If the device does have enough disk space but you prefer to save the database in an alternative location, you can use Migrate DB on the ELM Properties page to set up that location.

Migrate DB can be used at any time. However, if you migrate the management database once it contains records, the ELM session is on hold for several hours until the migration is complete, based on the number of records it contains. We recommend that you define this alternative location when you first set up the ELM device.

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

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click ELM Configuration | Migrate DB.
2. Select the storage device and a mirrored device.
3. Click OK.

Replace an ELM mirrored management database
If a mirrored management database storage device is having a problem, you might need to replace it.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the ELM device with the management database storage device that's experiencing the problem, then click the Properties icon.
2. Click ELM Configuration, then select Migrate DB.
3. In the Data Storage Devices field, select the device listed in the Mirrored Data Storage Device drop-down.
4. Select a new device in the Mirrored Data Storage Device field or select None to stop mirroring.

If the device you want isn't listed on the drop-down list, add the device to the Storage Device table first.
Retrieving ELM data
To retrieve data from the ELM, you must create search and integrity-check jobs on the Data page. An integrity-check job checks if the files that you define have been altered since they were originally stored. This can alert you to unauthorized modification of critical system or content files. The results of this check show which files were altered. If none of the files were altered, you are notified that the check was successful.

The system is limited to a total of 50 searches and integrity-check jobs at one time. If there are more than 50 on the system, you are informed that your search can't be performed. If you have existing searches on the system, you can delete them so that your new search can be performed. If you do not have existing searches, the system administrator deletes existing searches or integrity-check jobs initiated by other users for your search to be performed.

Once you initiate a search, it continues to run until it is complete or it reaches one of the limits you have set, even if you close the Data page. You can return to this screen to check on the status, which is displayed in the Search Results table.

Create a search job
To search the ELM for files that match your criteria, you must define a search job on the Data page. None of the fields on this screen are required; however, the better you are able to define your search, the more likely you are to retrieve the data you require in the least amount of time.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Data.
2. On the Search Logs and Files tab, fill in the information requested, then click Search.

Create an integrity-check job
You can check if files were altered since they were originally stored by creating an integrity-check job on the Data page. None of the fields on the Integrity Check tab are required; however, the better you are able to define your search, the more likely you are to verify the integrity of the data you require in the least amount of time.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select ELM Properties, then click Data.
2. Click the Integrity Check tab, make the requested selections, then click Search.

Advanced Correlation Engine (ACE) settings
McAfee Advanced Correlation Engine (ACE) identifies and scores threat events in real time, using both rule- and risk-based logic.

Identify what you value (users or groups, applications, specific servers, or subnets) and ACE alerts you if the asset is threatened. Audit trails and historical replays support forensics, compliance, and rule tuning.
Configure ACE using real-time or historical modes:

- **Real-time mode** — analyzes events as they are collected for immediate threat and risk detection.
- **Historical mode** — replays available data collected through either or both correlation engines for historical threat and risk detection. When ACE discovers new zero-day attacks, it determines whether your organization was exposed to that attack in the past, for subzero day threat detection.

ACE devices supplement the existing event correlation capabilities for ESM by providing two dedicated correlation engines. Configure each ACE device with its own policy, connection, event and log retrieval settings, and risk managers.

- **Risk correlation** — generates a risk score using rule-less correlation. Rule-based correlation only detects known threat patterns, requiring constant signature tuning and updates to be effective. Rule-less correlation replaces detection signatures with a one-time configuration: Identify what is important to your business (such as a particular service or application, a group of users, or specific types of data). **Risk Correlation** then tracks all activity related to those items, building a dynamic risk score that raises or lowers based on real-time activity.

  When a risk score exceeds a certain threshold, ACE generates an event and alerts you to growing threat conditions. Or, the traditional rule-based correlation engine can use the event as a condition of a larger incident. ACE maintains a complete audit trail of risk scores for full analysis and investigation of threat conditions over time.

- **Rule-based correlation** — detects threats using traditional rule-based event correlation to analyze collected information in real time. ACE correlates all logs, events, and network flows with contextual information, such as identity, roles, vulnerabilities, and more—to detect patterns indicative of a larger threat.

  Event Receivers support network-wide, rule-based correlation. ACE complements this capability with a dedicated processing resource that correlates larger volumes of data, either supplementing existing correlation reports or off-loading them completely.

Configure each ACE device with its own policy, connection, event and log retrieval settings, and risk managers.

**Select ACE data type**

ESM collects both event and flow data. Select which data to send to the ACE. Default is event data only.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select ACE Properties, then click ACE Configuration.
2. Click Data, then select Event Data, Flow Data, or both.
3. Click OK.

**Add a correlation manager**

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

**Before you begin**

There must be an ACE device on the ESM (see Add devices to the ESM console).
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select ACE Properties, then click Correlation Management.
2. Select the type of manager you want to create, then click OK.
3. If you selected Rule Correlation, complete the Main and Filters tabs. If you selected Risk Correlation, complete the Main, Fields, Thresholds, and Filters tabs.
4. Click Finish.

**Add a risk correlation manager**
You must add managers to help calculate the levels of risk for the fields that you designate.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select ACE Properties, then click Risk Correlation Management.
2. Click Add, then fill in the information requested on each tab.
3. Click Finish, then click Write to write the managers to the device.

**Add risk correlation score**
You must add conditional statements that assign a score to a targeted field.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select ACE Properties, then click Risk Correlation Scoring.
2. Click Add, then fill in the requested information.
3. Click OK.

**Using historical correlation**
The historical correlation option allows you to correlate past events.

When a new vulnerability is discovered, it's important to check your historical events and logs to see if you were exploited in the past. Using ACE's easy network replay feature, historical events can be played through the Risk Correlation rule-less correlation engine and through the standard rule-based event correlation engine, letting you examine historical events against today's threat landscape. This can be useful in these situations:

- You did not have correlation set up at the time certain events were triggered and you notice that correlating them might have revealed valuable information.
- You are setting up a new correlation based on events triggered in the past and you want to test the new correlation to confirm that it provides the desired results.

Be aware of the following when using historical correlation:

- Real-time correlation is discontinued until you disable historical correlation.
- The risk distribution is skewed by event aggregation.
- When you move the risk manager back to real-time risk correlation, the thresholds must be tuned.
To set up and run historical correlation you must:

1. Add a historical correlation filter.
2. Run a historical correlation.
3. Download and view the correlated historical events.

**Add and run historical correlation**
To correlate past events, you must set up an historical correlation filter, then run the correlation.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **ACE Properties**, then click **Historical**.
2. Click **Add**, fill in the information requested, then click **OK**.
3. Select **Enable Historical Correlation**, then click **Apply**.
   - Real-time correlation is discontinued until you disable historical correlation.
4. Select the filters you want to run, then click **Run Now**.

The ESM reviews the events, applies the filters, and packages the events that apply.

**Download and view the historical correlation events**
Once you have run the historical correlation, you can download and view the events it generated.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **ACE Properties**, then click **Events and Logs | Get Events**.
   - The events that resulted from running the historical correlation are downloaded to the ESM.
2. Close **ACE Properties**.
3. To view the data:
   a. On the system navigation tree, select the ACE device you just ran the historical data for.
   b. On the time period drop-down list on the view toolbar, select the period of time you specified when setting up the run.

The view pane displays the results of the query.

**Application Data Monitor (ADM) settings**
McAfee Application Data Monitor (ADM) tracks all use of sensitive data on the network, analyzing underlying protocols, session integrity, and application contents.

When ADM detects a violation, it preserves all details of that application session for use in incident response and forensics or for compliance audit requirements. At the same time, ADM provides visibility into threats that masquerade as legitimate applications.

ADM can detect when sensitive information is transmitted inside email attachments, instant messages, file transfers, HTTP posts, or other applications. Customize ADM’s detection capabilities by defining your own dictionaries of sensitive and confidential information. ADM can then detect these sensitive data types, alert appropriate personnel, and log the transgression to maintain an audit trail.
ADM monitors, decodes, and detects anomalies in the following application protocols:

- File transfer: FTP, HTTP, SSL (setup and certificates only)
- Email: SMTP, POP3, NNTP, MAPI
- Chat: MSN, AIM/Oscar, Yahoo, Jabber, IRC
- Webmail: Hotmail, Hotmail DeltaSync, Yahoo mail, AOL Mail, Gmail
- P2P: Gnutella, bitTorrent
- Shell: SSH (detection only), Telnet

ADM accepts rule expressions and tests them against monitored traffic, inserting records into the event table of the database for each triggered rule. It stores the packet that triggered the rule in the event table's packet field. It also adds application level metadata to the dbsession and query tables of the database for every triggered rule. It stores a text representation of the protocol stack in the query table's packet field.

ADM can generate the following types of event:

- **Metadata** - ADM generates one metadata event for each network transaction, with details such as addresses, protocol, file type, file name. The application places the metadata events in the query table and groups the events through the session table. For example, if one FTP session transfers three files, ADM groups them together.

- **Protocol anomaly** - Protocol anomalies are hard-coded into the protocol modules and include events, such as a Transmission Control Protocol (TCP) packet being too short to contain a valid header and a Simple Mail Transfer Protocol (SMTP) server returning an invalid response code. Protocol anomaly events are rare and are placed in the event table.

- **Rule trigger** - Rule expressions generate rule trigger events, detecting anomalies in the metadata generated by the Internet Communications Engine (ICE). These events might include anomalies such as protocols used outside of normal hours or an SMTP server unexpectedly talking FTP. Rule trigger events must be rare and are placed in the event table.

The event table contains one record for each detected protocol anomaly or rule trigger event. The event records link to the session and query tables through the sessionid, where more detail about the network transfers (metadata events) that triggered the event is available. Each event also links to the packet table where the raw packet data for the packet that triggered the event is available.

The session table contains one record for each group of related network transfers (such as, a group of FTP file transfers on the same session). The session records link to the query table through the sessionid where more details about the individual network transfers (metadata events) are found. In addition, if a transfer within the session causes a protocol anomaly or triggers a rule, there is a link to the event table.

The query table contains one record for each metadata event (content transfers that take place on the network). The query records link to the session table with the sessionid. If the network transfer represented by the record triggers a protocol anomaly or rule, there is a link to the event table. There is also a link to the packet table using the text field where a textual representation of the full protocol or content stack is found.

**Set ADM time zone**

The ADM device is set to GMT but ADM code is expecting the device to be set to your time zone. As a result, rules use the time trigger as if you are in GMT and not when you expect them to.

You can set the ADM to the time zone that you expect. This is then taken into account when evaluating the rules.
Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select ADM Properties, then click ADM Configuration.
2 Click Time Zone, then select your time zone.
3 Click OK.

Display password on Session Viewer
The Session Viewer allows you to see the details of the latest 25,000 ADM queries in a session. The rules for some of the events might be password-related. You can select whether you want the passwords to display on the Session Viewer. By default, passwords aren't displayed.

Task
For option definitions, click ? in the interface.

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

   The Passwords option states that logging is Off.
2 Click Passwords, select Enable password logging, then click OK.

   The system executes the command and informs you when it's completed.

The Passwords option now states that logging is On.

Application Data Monitor (ADM) dictionaries
When writing ADM rules, use dictionaries that translate keys captured from the network into a defined value. Or, list keys without a value that defaults to Boolean true when the keys are present. ADM dictionaries allow you to specify a file's keys quickly instead of having to write an individual rule for each word. For example, set up a rule to select email containing specific words, compile a dictionary with naughty words, and import that dictionary. You can create a rule like the following to check for emails with content that includes a word in the dictionary:

```
protocol == email && naughtyWords[objcontent]
```

When writing rules with the ADM rule editor, you can select the dictionary you want the rule to reference.

Dictionaries support up to millions of entries.

Adding a dictionary to a rule involves the following steps:
1 Setting up and saving a dictionary that lists the keys and, when needed, the values.
2 Managing the dictionary on the ESM.
3 Assigning the dictionary to a rule.

Setting up an ADM dictionary
A dictionary is a plain text file that consists of one entry per line. There are single column and double column dictionaries. Double columns include a key and a value.

Keys can be IPv4, MAC, number, regular expression, and string. Value types are boolean, IPv4, IPv6, MAC, number, and string. A value is optional and will default to boolean true if not present.
Values in a single or double column dictionary must be one of the supported ADM types: String, Regular Expression, Number, IPv4, IPv6, or MAC. ADM dictionaries must follow these formatting guidelines:

<table>
<thead>
<tr>
<th>Type</th>
<th>Syntax Rules</th>
<th>Examples</th>
<th>Content Matched</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>• Strings must be enclosed in double quotes</td>
<td>“Bad Content”</td>
<td>Bad Content</td>
</tr>
<tr>
<td></td>
<td>• Double quotes found within a String must be escaped</td>
<td>“He said, &quot;Bad Content&quot;”</td>
<td>He said, &quot;Bad</td>
</tr>
<tr>
<td></td>
<td>• Double quotes found within a String must be escaped using the backslash</td>
<td></td>
<td>Content</td>
</tr>
<tr>
<td></td>
<td>character before each quotation mark</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regular</td>
<td>• Regular expressions are enclosed with single forward slashes</td>
<td>/[Aa]pple/</td>
<td>Apple or apple</td>
</tr>
<tr>
<td>Expression</td>
<td>• Forward slashes and reserved regular expression characters within the</td>
<td>/apple/i</td>
<td>Apple or apple</td>
</tr>
<tr>
<td></td>
<td>regular expression must be escaped with the backslash character</td>
<td>/ [0-9]{1,3}.[0-9]{1,3}.[0-9].[0-9]/</td>
<td>IP Addresses:</td>
</tr>
<tr>
<td></td>
<td>• Can be written in standard dotted-quad notation</td>
<td>/1\2 of all/</td>
<td>1.1.1.1</td>
</tr>
<tr>
<td></td>
<td>• Can be written in CIDR notation</td>
<td></td>
<td>127.0.0.1</td>
</tr>
<tr>
<td></td>
<td>• Can be written in long format with full masks</td>
<td></td>
<td>1/2 of all</td>
</tr>
<tr>
<td>Numbers</td>
<td>• Decimal Values (0-9)</td>
<td>Decimal Value</td>
<td>123</td>
</tr>
<tr>
<td></td>
<td>• Hexadecimal Values (0x0-9a-f)</td>
<td>Hexadecimal Value</td>
<td>0x12ab</td>
</tr>
<tr>
<td></td>
<td>• Octal Values (0-7)</td>
<td>Octal Value</td>
<td>0127</td>
</tr>
<tr>
<td>Booleans</td>
<td>• Can be true or false</td>
<td>Boolean Literals</td>
<td>true</td>
</tr>
<tr>
<td></td>
<td>• All lower case</td>
<td></td>
<td>false</td>
</tr>
<tr>
<td>IPv4</td>
<td>• Can be written in standard dotted-quad notation</td>
<td>192.168.1.1</td>
<td>192.168.1.1</td>
</tr>
<tr>
<td></td>
<td>• Can be written in CIDR notation</td>
<td>192.168.1.0/24</td>
<td>192.168.1.0/24</td>
</tr>
<tr>
<td></td>
<td>• Can be written in long format with full masks</td>
<td>192.168.1.0/255.255.255.0</td>
<td>192.168.1.0/255.255.0</td>
</tr>
</tbody>
</table>

The following is true about dictionaries:

- Lists (multiple values separated by commas enclosed in brackets) are not allowed in dictionaries.
- A column can only consist of a single supported ADM type. This means that different types (string, regex, IPv4) cannot be mixed and matched within a single ADM dictionary file.
- They can contain comments. All lines starting with the pound character (#) are considered a comment within an ADM dictionary.
- Names can only consist of alphanumeric characters and underscores, and be of a total length less than or equal to 20 characters.
- Lists are not supported within them.
- Prior to ADM 8.5.0, they must be edited or created outside of the ESM with a text editor of your choice. They can be imported or exported from the ESM to facilitate modifying or creating new ADM dictionaries.
ADM dictionary examples

The ADM engine can match object content or any other metric or property with a single column dictionary for true or false (exists in the dictionary or does not exist in the dictionary).

Table 3-25  Single column dictionary examples

<table>
<thead>
<tr>
<th>Type of dictionary</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>String dictionary with common spam words</td>
<td>&quot;Cialis&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;cialis&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Viagra&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;viagra&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;adult web&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;Adult web&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;act now! don’t hesitate!&quot;</td>
</tr>
<tr>
<td>Regular expression dictionary for authorization key words</td>
<td>/(password</td>
</tr>
<tr>
<td></td>
<td>/(customer</td>
</tr>
<tr>
<td></td>
<td>/fund[^a-z0-9]{1,3}transaction/i</td>
</tr>
<tr>
<td></td>
<td>/fund[^a-z0-9]{1,3}transfer[^a-z0-9]{1,3}[0-9,]+/i</td>
</tr>
<tr>
<td>String dictionary containing hash values for known bad executables</td>
<td>&quot;fec72ceae15b6f60cbf269f99b9888e9&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;fed472c13c1db095c4cb0fc54ed28485&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;feddedb607468465f9428a59eb5ee22a&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;ff3cb87742f9b56d6db9a49b31c1743c&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;ff45e471aa68c9e2b6d62a82b6b6a82a&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;ff669082fa0b5b976cec8027833791c&quot;</td>
</tr>
<tr>
<td></td>
<td>&quot;ff7025e261bd09250346bc9efdfc6c7c&quot;</td>
</tr>
<tr>
<td>IP addresses of critical assets</td>
<td>192.168.1.12</td>
</tr>
<tr>
<td></td>
<td>192.168.2.0/24</td>
</tr>
<tr>
<td></td>
<td>192.168.3.0/255.255.255.0</td>
</tr>
<tr>
<td></td>
<td>192.168.4.32/27</td>
</tr>
<tr>
<td></td>
<td>192.168.5.144/255.255.255.240</td>
</tr>
</tbody>
</table>
### Table 3-26  Double column dictionary examples

<table>
<thead>
<tr>
<th>Type of dictionary</th>
<th>Example</th>
</tr>
</thead>
</table>
| String dictionary with common spam words and categories | “Cialis” “pharmaceutical”  
“cialis” “pharmaceutical”  
“Viagra” “pharmaceutical”  
“viagra” “pharmaceutical”  
“adult web” “adult”  
“Adult web” “adult”  
“act now! don’t hesitate!” “scam” |
| Regular expression dictionary for authorization key words and categories | /*(password|passwd|pwd)[^a-z0-9]{1,3}(admin|login|password|user)/i “credentials”  
/(customer|client)[^a-z0-9]{1,3}account[^a-z0-9]{1,3}number/i “pii”  
/fund[^a-z0-9]{1,3}transaction/i “sox”  
/fund[^a-z0-9]{1,3}transfer[^a-z0-9]{1,3}[0-9,].+*/i “sox” |
| String dictionary containing hash values for known bad executables and categories | "fec72ceae15b66f60cbf269f99b9888e9" “Trojan”  
"fed472c13c1db095c4cb0cf54ed28485" "Malware”  
"feddedb607468465f9428a59eb5ee22a" “Virus”  
"ff3cb87742f9b56dfdb9a49b31c1743c" “Malware”  
"ff45e471aa68c9e2b6d62a82bb6a82a" “Adware”  
"ff669082fa0b5b976cecc8027833791c" “Trojan”  
"ff7025e261bd09250346bc9efdfc6c7c" “Virus” |
| IP addresses of critical assets & groups | 192.168.1.12 “Critical Assets”  
192.168.2.0/24 “LAN”  
192.168.3.0/255.255.255.0 “LAN”  
192.168.4.32/27 “DMZ”  
192.168.5.144/255.255.255.240 “Critical Assets” |

### Manage ADM dictionaries

Once you set up and save a new dictionary, you must import it to the ESM. You can also export, edit, and delete it.

**Task**

For option definitions, click ? in the interface.

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

   The Manage ADM Dictionaries screen lists the four default dictionaries (botnet, foulanguage, icd9_desc, and spamlist) and any dictionaries that were imported to the system.

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

### Reference an ADM dictionary

When a dictionary is imported to the ESM, you can refer to it when writing rules.

**Before you begin**

Import the dictionary to the ESM.
**Task**
For option definitions, click ? in the interface.

1. In the Rule Types pane of the Policy Editor, click New | ADM Rule.
2. Add the requested information and drag-and-drop a logical element to the Expression Logic area.
3. Drag-and-drop the Expression Component icon on the logical element.
4. On the Expression Component page, select the dictionary in the Dictionary field.
5. Fill in the remaining fields, then click OK.

**ADM rule reference material**
This appendix includes material that can assist you when adding ADM rules to the Policy Editor.

**ADM rules syntax**
The ADM rules are very similar to C expressions.

The main difference is a more extensive set of literals (numbers, strings, regular expressions, IP addresses, MAC addresses, and Booleans). String terms can be compared with string and Regex literals to test their content but they can also be compared with numbers to test their length. Numeric, IP address, and MAC address terms can only be compared with the same type of literal value. The only exception is that everything can be treated as a Boolean to test for its existence. Some terms can have multiple values, for example the following rule would trigger for PDF files inside .zip files: type = application/zip && type = application/pdf.

<table>
<thead>
<tr>
<th>Table 3-27 Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
</tr>
<tr>
<td>&amp;&amp;</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>^ ^</td>
</tr>
<tr>
<td>!</td>
</tr>
<tr>
<td>= =</td>
</tr>
<tr>
<td>! =</td>
</tr>
<tr>
<td>&gt;</td>
</tr>
<tr>
<td>&gt; =</td>
</tr>
<tr>
<td>&lt;</td>
</tr>
<tr>
<td>&lt; =</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3-28 Literals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Literal</td>
</tr>
<tr>
<td>Number</td>
</tr>
<tr>
<td>String</td>
</tr>
<tr>
<td>Regex</td>
</tr>
<tr>
<td>IPv4</td>
</tr>
</tbody>
</table>
### Table 3-28 Literals (continued)

<table>
<thead>
<tr>
<th>Literal</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>aa:bb:cc:dd:ee:ff</td>
</tr>
<tr>
<td>Bool</td>
<td>true, false</td>
</tr>
</tbody>
</table>

### Table 3-29 Type operator compatibility

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

### Table 3-30 ADM regex grammar

#### Basic operators

| | Alternation (or) |
| | Zero or more |
| | One or more |
| | Zero or one |
| | Grouping (a | b) |
| | Repeating Range {x} or {.x} or {x,} or {x,y} |
| | Range [0-9a-z] [abc] |
| | Exclusive Range [^abc] [^0-9] |
| | Any Character |
| | Escape Character |

#### Escapes

| \d | Digit [0-9] |
| \D | Non-Digit [^0-9] |
| \e | Escape (0x1B) |
| \f | Form Feed (0x0C) |
| \n | Line Feed (0x0A) |
| \r | Carriage Return (0x0D) |
| \s | White Space |
| \S | Not White Space |
**Escapes**

<table>
<thead>
<tr>
<th>Esc</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\t</td>
<td>Tab (0x09)</td>
</tr>
<tr>
<td>\v</td>
<td>Vertical Tab (0x0B)</td>
</tr>
<tr>
<td>\w</td>
<td>Word [A-Za-z0-9_]</td>
</tr>
<tr>
<td>\W</td>
<td>Not Word</td>
</tr>
<tr>
<td>\x00</td>
<td>Hex Representation</td>
</tr>
<tr>
<td>\0000</td>
<td>Octal Representation</td>
</tr>
<tr>
<td>^</td>
<td>Start of line</td>
</tr>
<tr>
<td>S</td>
<td>End of line</td>
</tr>
</tbody>
</table>

- The start of line and end of line anchors (^ and $) don’t work for objcontent.

**POSIX character classes**

<table>
<thead>
<tr>
<th>Class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:alnum:]</td>
<td>Digits and letters</td>
</tr>
<tr>
<td>[:alpha:]</td>
<td>All letters</td>
</tr>
<tr>
<td>[:ascii:]</td>
<td>ASCII Characters</td>
</tr>
<tr>
<td>[:blank:]</td>
<td>Space and tab</td>
</tr>
<tr>
<td>[:cntrl:]</td>
<td>Control characters</td>
</tr>
<tr>
<td>[:digit:]</td>
<td>Digits</td>
</tr>
<tr>
<td>[:graph:]</td>
<td>Visible characters</td>
</tr>
<tr>
<td>[:lower:]</td>
<td>Lowercase letters</td>
</tr>
<tr>
<td>[:print:]</td>
<td>Visible characters and spaces</td>
</tr>
<tr>
<td>[:punct:]</td>
<td>Punctuation and Symbols</td>
</tr>
<tr>
<td>[:space:]</td>
<td>All whitespace characters</td>
</tr>
<tr>
<td>[:upper:]</td>
<td>Uppercase characters</td>
</tr>
<tr>
<td>[:word:]</td>
<td>Word characters</td>
</tr>
<tr>
<td>[:xdigit:]</td>
<td>Hexadecimal Digit</td>
</tr>
</tbody>
</table>

**ADM rule term types**

All terms in an ADM rule have a specific type. Each term is either an IP address, a MAC address, a number, a string, or a boolean. In addition there are two extra literal types: regular expressions and lists. A term of a specific type can generally only be compared against a literal of the same type or a list of literals of the same type (or a list of lists of ...). There are three exceptions to this rule:
1. A string term can be compared against a numeric literal to test its length. The following rule triggers if a password is fewer than eight characters long (password is a string term): `password < 8`

2. A string term can be compared against a regular expression. The following rule triggers if a password only contains lower case letters: `password == /^[a-z]+$/`

3. All terms can be tested against boolean literals to test whether they occur at all. The following rule triggers if an email has a CC address (email.cc is a string term): `email.cc == true`

<table>
<thead>
<tr>
<th>Type</th>
<th>Format description</th>
</tr>
</thead>
</table>
| 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 ADM rules are 32-bit integers. They can be written in decimal: 1234  
|                  | • They can be written in hexadecimal: 0xabcd  
|                  | • They can be written in octal: 0777  
|                  | • They can have a multiplier appended to multiply by 1024 (K), 1048576 (M) or 1073741824 (G): 10M  |
| Strings          | • Strings are enclosed in double quotes: "this is a string"  
|                  | • Strings can use standard C escape sequences: "\tThis is a "string"\n" containing \x20escape sequences\n"  
|                  | • When comparing a term against a string, the whole term must match the string. If an email message has a from address of someone@somewhere.com then the following rule will not trigger: `email.from == "@somewhere.com"`  
|                  | • To match only a part of a term, a regular expression literal should be used instead. String literals must be used when possible because they are more efficient.  |
| Booleans         | • The boolean literals are true and false.  |

All email address and URL terms are normalized before matching so it is not necessary to take account of things like comments within email addresses.
### 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]+/`
- Regular expressions can be followed by standard modifier flags, though "i" is the only one currently recognized (case-insensitive): `/[a-z]+/i`
- Regular expression literals should use the POSIX Extended syntax. Currently Perl extensions work for all terms except the content term but this might change in future versions.
- When comparing a term against a regular expression, the regular expression matches any substring within the term unless anchor operators are applied within the regular expression. The following rule triggers if an email is seen with an address of “someone@somewhere.com”: 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 kind of literal, it’s not valid to mix strings and numbers, strings and regular expressions, IP addresses and MAC addresses.
- When a list is used with any relational operator other than not-equal (!=), 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 of the literals in the list. The following rule triggers if the source IP address is not 192.168.1.1 or 192.168.1.2: 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 a lot of sense. The following rule triggers if the object size is greater than 100 or if the object size is greater than 200: objectsize > [100, 200]
  - It is equivalent to: objectsize > 100 || objectsize > 200

### ADM rule metric references

Here are lists of metric references for ADM rule expressions, which are available on the Expression Component page when you are adding an ADM rule.

For Common Properties and Common Anomalies, the parameter-type value you can enter for each one is shown in parentheses after the metric reference.

#### Common Properties

<table>
<thead>
<tr>
<th>Property or term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol (Number)</td>
<td>The application protocol (HTTP, FTP, SMTP)</td>
</tr>
<tr>
<td>Object Content (String)</td>
<td>The content of an object (text inside a document, email message, chat message). Content matching is not available for binary data. Binary objects can, however, be detected using Object Type (objtype)</td>
</tr>
<tr>
<td>Object Type (Number)</td>
<td>Specifies the type of the content as determined by ADM (Office Documents, Messages, Videos, Audio, Images, Archives, Executables)</td>
</tr>
<tr>
<td>Object Size (Number)</td>
<td>Size of the object. Numeric multipliers K, M, G can be added after the number (10K, 10M, 10G)</td>
</tr>
<tr>
<td>Property or term</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Object Hash (String)</td>
<td>The hash of the content (currently MD5)</td>
</tr>
<tr>
<td>Object Source IP Address (Number)</td>
<td>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</td>
</tr>
<tr>
<td>Object Destination IP Address (Number)</td>
<td>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</td>
</tr>
<tr>
<td>Object Source Port (Number)</td>
<td>The source TCP/UDP port of the content</td>
</tr>
<tr>
<td>Object Destination Port (Number)</td>
<td>The destination TCP/UDP port of the content</td>
</tr>
<tr>
<td>Object Source IP v6 Address (Number)</td>
<td>The source IPv6 address of the content</td>
</tr>
<tr>
<td>Object Destination IPv6 Address (Number)</td>
<td>The destination IPv6 address of the content</td>
</tr>
<tr>
<td>Object Source MAC Address (mac name)</td>
<td>The source MAC address of the content (aa:bb:cc:dd:ee:ff)</td>
</tr>
<tr>
<td>Object Destination MAC Address (mac name)</td>
<td>The destination MAC address of the content (aa:bb:cc:dd:ee:ff)</td>
</tr>
<tr>
<td>Flow Source IP Address (IPv4)</td>
<td>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</td>
</tr>
<tr>
<td>Flow Destination IP Address (IPv4)</td>
<td>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</td>
</tr>
<tr>
<td>Flow Source Port (Number)</td>
<td>Source TCP/UDP port of flow</td>
</tr>
<tr>
<td>Flow Destination Port (Number)</td>
<td>Destination TCP/UDP port of flow</td>
</tr>
<tr>
<td>Flow Source IPv6 Address (Number)</td>
<td>Source IPv6 address of the flow</td>
</tr>
<tr>
<td>Flow Destination IPv6 Address (Number)</td>
<td>Destination IPv6 address of the flow</td>
</tr>
<tr>
<td>Flow Source MAC Address (mac name)</td>
<td>Source MAC address of the flow</td>
</tr>
<tr>
<td>Flow Destination MAC Address (mac name)</td>
<td>Destination MAC address of flow</td>
</tr>
<tr>
<td>VLAN (Number)</td>
<td>Virtual LAN ID</td>
</tr>
<tr>
<td>Day of Week (Number)</td>
<td>The day of the week. Valid values are 1–7; 1 is Monday.</td>
</tr>
<tr>
<td>Hour of Day (Number)</td>
<td>The hour of the day set to GMT. Valid values are 0–23.</td>
</tr>
<tr>
<td>Declared Content Type (String)</td>
<td>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.</td>
</tr>
<tr>
<td>Password (String)</td>
<td>Password used by the application for authentication.</td>
</tr>
<tr>
<td>URL (String)</td>
<td>Website URL. Applies only to HTTP protocol.</td>
</tr>
<tr>
<td>File Name (String)</td>
<td>Name of the file being transferred.</td>
</tr>
<tr>
<td>Display Name (String)</td>
<td>Host name as specified in DNS lookup.</td>
</tr>
<tr>
<td>Host Name (String)</td>
<td></td>
</tr>
</tbody>
</table>
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, ADM also provides protocol-specific properties that can be used with ADM rules. All protocol-specific properties are also available in the Expression Component page when adding an ADM rule.

Examples of protocol-specific properties

These properties apply to these tables:

* Detection only
** No decryption, captures X.509 certificates and encrypted data
*** Via RFC822 module

Table 3-31  File transfer protocol modules

<table>
<thead>
<tr>
<th>FTP</th>
<th>HTTP</th>
<th>SMB*</th>
<th>SSL**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Display Name</td>
<td>Display Name</td>
<td>Display Name</td>
</tr>
<tr>
<td>File Name</td>
<td>File Name</td>
<td>File Name</td>
<td>File Name</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host Name</td>
<td>Host Name</td>
<td>Host Name</td>
</tr>
<tr>
<td>URL</td>
<td>Referer</td>
<td>URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>All HTTP headers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3-32  Email protocol modules

<table>
<thead>
<tr>
<th>DeltaSync</th>
<th>MAPI</th>
<th>NNTP</th>
<th>POP3</th>
<th>SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bcc***</td>
<td>Bcc</td>
<td>Bcc***</td>
<td>Bcc***</td>
<td>Bcc***</td>
</tr>
<tr>
<td>Cc***</td>
<td>Cc</td>
<td>Cc***</td>
<td>Cc***</td>
<td>Cc***</td>
</tr>
<tr>
<td>Display Name</td>
<td>Display Name</td>
<td>Display Name</td>
<td>Display Name</td>
<td>Display Name</td>
</tr>
<tr>
<td>From***</td>
<td>From***</td>
<td>From***</td>
<td>From***</td>
<td>From***</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host Name</td>
<td>Host Name</td>
<td>Host Name</td>
<td>Host Name</td>
</tr>
<tr>
<td>Subject***</td>
<td>Subject***</td>
<td>Subject***</td>
<td>Subject***</td>
<td>Subject***</td>
</tr>
<tr>
<td>To***</td>
<td>To***</td>
<td>To***</td>
<td>To***</td>
<td>To***</td>
</tr>
<tr>
<td></td>
<td>User Name</td>
<td></td>
<td>User Name</td>
<td>User Name</td>
</tr>
</tbody>
</table>
Protocol anomalies

Beyond the common properties and protocol-specific properties, ADM also detects hundreds of anomalies in low-level, transport, and application protocols. All protocol anomaly properties are of type Boolean and are available in the Expression Component page when you are adding an ADM rule.

Table 3-34  IP

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip.too-small</td>
<td>IP packet is too small to contain a valid header.</td>
</tr>
<tr>
<td>ip.bad-offset</td>
<td>IP data offset goes past end of packet.</td>
</tr>
<tr>
<td>ip.fragmented</td>
<td>IP packet is fragmented.</td>
</tr>
<tr>
<td>ip.bad-checksum</td>
<td>IP packet checksum doesn't match data.</td>
</tr>
<tr>
<td>ip.bad-length</td>
<td>IP packet totlen field goes past end of packet.</td>
</tr>
</tbody>
</table>

Table 3-35  TCP

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp.too-small</td>
<td>TCP packet is too small to contain a valid header.</td>
</tr>
<tr>
<td>tcp.bad-offset</td>
<td>TCP packet's data offset goes past end of packet.</td>
</tr>
<tr>
<td>tcp.unexpected-fin</td>
<td>TCP FIN flag set in non-established state.</td>
</tr>
<tr>
<td>tcp.unexpected-syn</td>
<td>TCP SYN flag set in established state.</td>
</tr>
<tr>
<td>tcp.duplicate-ack</td>
<td>TCP packet ACKs data that's already been ACKed.</td>
</tr>
<tr>
<td>tcp.segment-outsidewindow</td>
<td>TCP packet is outside the window (TCP module’s small window, not real window).</td>
</tr>
<tr>
<td>tcp.urgent-nonzero-withouturg-flag</td>
<td>TCP urgent field is non-zero but URG flag isn't set.</td>
</tr>
</tbody>
</table>

Table 3-36  DNS

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.too-small</td>
<td>DNS packet is too small to contain a valid header.</td>
</tr>
<tr>
<td>dns.question-name-past-end</td>
<td>DNS question name goes past the end of the packet.</td>
</tr>
</tbody>
</table>
Table 3-36  DNS (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns.answer-name-past-end</td>
<td>DNS answer name goes past the end of the packet.</td>
</tr>
<tr>
<td>dns.ipv4-address-length-wrong</td>
<td>IPv4 address in DNS response is not 4 bytes long.</td>
</tr>
</tbody>
</table>

Database Event Monitor (DEM) settings

McAfee Database Event Monitor (DEM) consolidates database activity into a central audit repository and provides normalization, correlation, analysis, and reporting of that activity. If network or database server activity matches known patterns indicating malicious data access, DEM generates an alert. In addition, all transactions are logged for use in compliance.

DEM enables you to manage, edit, and adjust database monitoring rules from the same interface that provides analysis and reporting. You can easily adjust specific database monitoring profiles (which rules are enforced, what transactions are logged), reducing false-positives and improving security overall.

DEM non-intrusively audits the interactions of your users and applications with your databases by monitoring network packets similar to intrusion detection systems. To ensure that you can monitor all database server activity over the network, coordinate your initial DEM deployment with your networking, security, compliance, and database teams.

Your network teams use span ports on switches, network taps, or hubs to replicate database traffic. This process allows you to listen to or monitor the traffic on your database servers and create an audit log.

Visit the McAfee website for information about supported database server platforms and versions.

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Database</th>
<th>DEM appliance</th>
<th>DEM agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows, UNIX/Linux (all versions)</td>
<td>Oracle²</td>
<td>Oracle 8.x, 9.x, 10 g, 11 g R2²</td>
<td>Oracle 8.0.3+, 9.x, 10.x, 11.x</td>
</tr>
<tr>
<td></td>
<td>Sybase</td>
<td>11.x, 12.x, 15.x</td>
<td>11.x, 12.x, 15.x</td>
</tr>
<tr>
<td></td>
<td>DB2</td>
<td>8.x, 9.x, 10.x</td>
<td>7.1.x, 8.x, 9.x</td>
</tr>
<tr>
<td></td>
<td>Informix (available in 8.4.0 and later)</td>
<td>11.5</td>
<td>--</td>
</tr>
<tr>
<td>Windows, UNIX/Linux (all versions)</td>
<td>MySQL</td>
<td>Yes, 4.x, 5.x, 6.x</td>
<td>Yes, 4.1.22.x, 5.0.3x</td>
</tr>
<tr>
<td></td>
<td>PostgreSQL</td>
<td>7.4.x, 8.4.x, 9.0.x, 9.1.x</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>Teradata</td>
<td>12.x, 13.x, 14.x</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>InterSystems Cache</td>
<td>2011.1.x</td>
<td>--</td>
</tr>
<tr>
<td>UNIX/Linux (all versions)</td>
<td>Greenplum</td>
<td>8.2.15</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>Vertica</td>
<td>5.1.1-0</td>
<td>--</td>
</tr>
<tr>
<td>Mainframe</td>
<td>DB2/zOS</td>
<td>All versions</td>
<td>Partner agent option</td>
</tr>
</tbody>
</table>
### Operating system | Database | DEM appliance | DEM agent
---|---|---|---
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 11g is available in version 8.3.0 and later.

The following applies to these servers and versions:

- Both 32-bit and 64-bit versions of operating systems and database platforms are supported.
- MySQL is supported on Windows 32-bit platforms only.
- Packet decryption is supported for MSSQL and Oracle.

### Update DEM license
The DEM comes with a default license. If you change the capabilities of the DEM, McAfee sends you a new license in an email message and you must update it.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.
2. Click **License | Update License**, then paste the information sent to you by McAfee in the field.
3. Click **OK**.
   - The system updates the license and informs you when it’s done.
4. Roll out the policy to the DEM.

### Sync DEM configuration files
When DEM configuration files are out of sync with the DEM device, you must write the configuration files to the DEM.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.
2. Click **Sync Files**.
   - A message displays the status of the sync.

### Configure advanced DEM settings
These advanced settings change or increase the performance of the DEM.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **DEM Properties**, then click **DEM Configuration**.
2. Click **Advanced**, then define the settings or deselect options if you begin to experience a heavy load on the DEM.
3. Click **OK**.
Apply DEM configuration settings
Changes made to DEM configuration settings must be applied to the DEM. Should you neglect to apply any configuration changes, the Apply option on DEM Configuration allows you to do so for all DEM configuration settings.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select DEM Properties, then click DEM Configuration.
2. Click Apply.

A message informs you when the configuration settings are written to the DEM.

Defining actions for DEM events
Action Management settings on the DEM define actions and operations for events, which are used in the DEM’s filtering rules and data access policies. You can add custom actions and set the Operation for default and custom actions.

The DEM comes with default actions, which you can see by clicking Edit Global on the Action Management page, and these default operations:

- none
- scripts
- ignore
- reset
- discard

If you select Script as the operation, an alias name (SCRIPT ALIAS) is required, pointing to the actual script (SCRIPT NAME) that must be executed when the criticality event occurs. The script is passed two environment variables, ALERT_EVENT and ALERT_REASON. ALERT_EVENT contains a colon-separated list of metrics. DEM provides a sample bash script /home/auditprobe/conf/sample/process_alerts.bash to demonstrate how the criticality action can be captured in a script.

When working with actions and operations, keep this in mind:

- Actions are listed in order of priority.
- An event does not take an action such as sending an SNMP trap or page unless you specify this as the alert action.
- When a rule qualifies for more than one alert level, only the highest alert level is actionable.
- Events are written to an event file regardless of the action. The only exception is a Discard operation.

Add a DEM action
If you add an action to DEM action management, it appears on the list of available actions for a DEM rule in the Policy Editor. You can then select it as the action for a rule.

Task
For option definitions, click ? in the interface.

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

The DEM Action Management page lists the existing actions in order of priority.

You can’t change the priority order of the default actions.
2 Click **Add**, then enter a name and description for this action.

You can't delete a custom action once it's added.

3 Click **OK**.

The new action is added to the **DEM Action Management** list.

The default operation for a custom action is **None**. To change this, see *Set the operation for a DEM action*.

**Edit a DEM custom action**

Once you have added an action to the DEM action management list, you might need to edit its name or change its priority.

**Task**

For option definitions, click ? in the interface.

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

2 Click the custom action you need to change and do one of the following:
   - To change the priority order, click the up or down arrows until it is in the correct position.
   - To change the name or description, click **Edit**.

3 Click **OK** to save your settings.

**Set the operation for a DEM action**

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

**Task**

For option definitions, click ? in the interface.

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

2 Highlight the action you want to edit, then click **Edit**.

3 Select an operation, then click **OK**.

**Working with sensitive data masks**

Sensitive data masks prevent unauthorized viewing of sensitive data by replacing the sensitive information with a generic string, called the mask. Three standard sensitive data masks are added to
the ESM database when you add a DEM device to the system, but you can add new ones and edit or remove existing ones.

These are the standard masks:

- **Sensitive mask name: Credit Card Number Mask**
  
  **Expression:** ((4\d\{3\})(5\[1-5]\d\{2\})|(6011))-?\d\{4\}-?\d\{4\}-?\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+identified\s+by\s+\(\w+\)
  
  **Substring Index:** \2
  
  **Masking Pattern:** ********

**Manage sensitive data masks**

To protect sensitive information entered on the system, you can add sensitive data masks and edit or remove existing ones.

**Task**

For option definitions, click ? in the interface.

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

2. Select an option, then enter the requested information.

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

Much of security is based on a simple principle that users have to be identified and distinguished from each other, yet generic user names are often used to access the database. Identifier management provides a way to capture the real user name if it exists anywhere in the query, using REGEX patterns. Applications can be quite easily instrumented to take advantage of this security feature. Two defined identifier rules are added to the ESM database when you add a DEM device to the system.

- **Identifier Rule Name: Get User Name from SQL Stmt**
  
  Expression: `select\s+username=(\w+)`

  Application: Oracle

  Substring Index: \1

- **Identifier Rule Name: Get User Name from Stored Procedure**

  Expression: `sessionStart\s+@appname='(\w+)', @username='(\w+)'

  Application: MSSQL

  Substring Index: \2

Advanced user correlation is possible by correlating the DEM, application, web server, system, and identity and access management logs in the ESM.

Add a user identifier rule

To associate database queries with individuals, you can use the existing user identifier rules or add a new rule.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **DEM Properties**, then click **Identifier Management**.
2. Click **Add**, then enter the information requested.
3. Click **OK**, then click **Write** to write the settings to the DEM.

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:

<table>
<thead>
<tr>
<th>OS</th>
<th>Database</th>
<th>DEM Appliance</th>
<th>DEM Agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows UNIX/Linux (all versions)</td>
<td>Oracle²</td>
<td>Oracle 8.x, 9.x, 10g, 11g³, 11g R2</td>
<td>Oracle 8.0.3+, 9.x, 10.x, 11.x</td>
</tr>
<tr>
<td></td>
<td>Sybase</td>
<td>11.x, 12.x, 15.x</td>
<td>11.x, 12.x, 15.x</td>
</tr>
<tr>
<td></td>
<td>DB2</td>
<td>8.x, 9.x, 10.x</td>
<td>7.1.x, 8.x, 9.x</td>
</tr>
<tr>
<td></td>
<td>Informix (see note 4)</td>
<td>11.5</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>MySQL</td>
<td>Yes, 4.x, 5.x, 6.x</td>
<td>Yes, 4.1.22.x, 5.0.3x</td>
</tr>
</tbody>
</table>
### OS | Database | DEM Appliance | DEM Agent
--- | --- | --- | ---
 | 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 | Partner agent option |
 | 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.
- DEM agents are supported on all OS versions of Windows, UNIX, and Linux.
- DEM agents require java virtual machine (JVM).
- MySQL is supported on Windows 32-bit platforms only.
- Packet decryption is supported for MSSQL & Oracle.

### Manage database servers

The Database Server page is the starting point for managing settings for all database servers for your DEM device.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select DEM Properties, then click Database Servers.
2. Select any of the available options.
3. Click OK.

### Manage database discovery notifications

The DEM has a database discovery feature that provides an exception list of database servers that are not being monitored. This allows a security administrator to discover new database servers added to the environment and illegal listener ports opened to access data from databases. When this is enabled, you receive an alert notification that shows up on the Event Analysis view. You can then choose whether to add the server to those being monitored on your system.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select DEM Properties, then click Database Servers | Enable.
   - You are notified when it's enabled.
2. Click OK to close DEM Properties.
To view the notifications, click the DEM device on the system navigation tree, then select Event Views | Event Analysis.

To add the server to your system, select the Event Analysis view, then click the Menu icon and select Add Server.

**Distributed ESM (DESM) settings**

Distributed ESM (DESM) provides a distributed architecture that allows a parent ESM to connect to and gather data from up to 100 devices. The parent pulls data from the device based on filters that you define. In addition, you can seamlessly drill down to data that originated and remains on the device ESM.

The DESM must approve the parent ESM to allow it to pull events. The parent can set filters, sync data sources, and push its custom types. It can't get rules or events from the DESM until it is approved.

If you log on with administrator rights to the DESM, a notification appears stating, "This ESM has been added as a Distributed ESM on another server. Waiting for approval to connect." When you click Approve Hierarchical ESMs, you can select the type of communication the parent ESM can have with the DESM.

The parent ESM doesn't manage devices belonging to device ESM. The parent ESM shows the System Tree of the device ESM to which it is directly connected. It does not pull events from or display any of the devices' child ESM. Toolbars are disabled for all DESM children.

The parent does not manage data that resides on device ESM. Instead, a subset of the device from the ESM data is transferred and stored on the parent ESM, based on the filters you define.

**Add DESM filters**

Data transferred from the device ESM to the parent DESM depend on user-defined filters. When these filters are saved, it's equivalent to applying the filter on the device ESM, so the appropriate hashes or bitsets can be generated. Because the purpose of the DESM feature is to allow you to gather specific data from the device ESM (not ALL data), you must set filters for data to be retrieved from the device ESM.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select DESM Properties, then click Filters.
2. Enter the requested data, then click OK.

**ePolicy Orchestrator settings**

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

You must associate the ePolicy Orchestrator with a Receiver because the events are pulled from the Receiver, not ePolicy Orchestrator.

You must have read permissions on the master database and ePolicy Orchestrator database to use ePolicy Orchestrator.

If the McAfee ePO device has a McAfee Threat Intelligence Exchange server, it is added automatically when you add the McAfee ePO device to the ESM (see Threat Intelligence Exchange integration).
Launch ePolicy Orchestrator

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

Before you begin
Add an ePolicy Orchestrator device or data source to the ESM.

This feature is available on ePolicy Orchestrator 4.6 and later.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select a view.
2. Select a result from a bar, list, pie, graph, or table component that returns source IP or destination IP data.
3. On the component's menu, click Action | Launch ePO.
   - If you only have one ePolicy Orchestrator device or data source on the system and you selected a source IP or destination IP in Step 1, ePolicy Orchestrator launches.
   - If you have more than one ePolicy Orchestrator device or data source on the system, select the one you want to access and ePolicy Orchestrator launches.
   - If you selected an event or flow on a table component in Step 1, select whether you want to access the source IP or destination IP address, then ePolicy Orchestrator launches.

McAfee ePO device authentication

Authentication is required before using McAfee ePO tagging or actions, or McAfee Real Time for McAfee ePO.

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, tags, or McAfee Real Time for McAfee ePO, use the selected method of authentication. If the credentials aren't found or are invalid, you are prompted to enter valid credentials, which you must save for future communication with the device.

Running reports, data enrichment, and dynamic watchlists in the background through McAfee Real Time for McAfee ePO uses the originally supplied McAfee ePO credentials.

Setting up separate account authentication

Global account authentication is the default setting. There are two things you must do to set up separate account authentication.

1. Verify that Require user authentication is selected when adding the McAfee ePO device to the ESM or when you set up its connection settings (see Add devices to the ESM console or Change connection with ESM).
2. Enter your credentials on the Options page (see Add McAfee ePO authentication credentials).
Add McAfee ePO authentication credentials
Before using McAfee ePO tagging or actions, or McAfee Real Time for McAfee ePO, you must add the authentication credentials to the ESM.

Before you begin
Install a McAfee ePO device on the ESM (see Add devices to the ESM console).
Contact your system administrator if you don't have the user name and password for the device.

Task
For option definitions, click ? in the interface.
1 On the system navigation bar of the ESM console, click options, then click ePO Credentials.
2 Click the device, then click Edit.
3 Provide the user name and password, then click Test Connection.
4 Click OK.

Assign ePolicy Orchestrator tags to IP address
The ePO Tagging tab lists the available tags. You can assign tags to events generated by an alarm and view if an alarm has ePolicy Orchestrator tags. You can also select one or more tags on this page and apply them to an IP address.

To access the tagging functionality, you must have the Apply, exclude, and clear tags and Wake up agents; view Agent Activity Log permissions on ePolicy Orchestrator.

Task
For option definitions, click ? in the interface.
1 On the system navigation tree, select ePO Properties, then click Tagging.
2 Complete the requested information, then click Assign.
The selected tags are applied to the IP address.

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

When you add ePolicy Orchestrator, you are asked if you want to configure McAfee Risk Advisor data. If you click Yes, a data enrichment source and two ACE scoring rules (if applicable) are created and rolled out. To view these, go to the Data Enrichment and Risk Correlation Scoring pages. If you want to use the scoring rules, you must create a risk correlation manager.

Enable McAfee Risk Advisor data acquisition
When you enable McAfee Risk Advisor data acquisition on ePolicy Orchestrator, a score list is generated and sent to any ACE device to be used for scoring SrcIP and DstIP fields.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select ePO Properties | Device Management, then click Enable.
   - You are informed when acquisition is enabled.
2. Click OK.

**Perform McAfee Real Time for McAfee ePO actions**
Execute McAfee Real Time for McAfee ePO actions on the results of a question from the ESM and component that display an IP address in the view.

### Before you begin
- Design and run a McAfee Real Time for McAfee ePO question (see Query McAfee ePO for McAfee Real Time for McAfee ePO dashboard).

**Task**
For option definitions, click ? in the interface.

1. On the ESM console, click the menu icon on a view component that shows the results of a McAfee Real Time for McAfee ePO question.
2. Highlight Actions, then click Real Time for ePO Actions.
3. On the Devices tab, select the McAfee ePO device to perform the action on.
4. On the Actions tab, click an action from the list of available actions for the selected devices.
5. On the Filters tab, specify a set of filters to apply to the question, then click Finish.
   - Filters aren’t available from the McAfee ePO dashboard or components.

**Threat Intelligence Exchange integration**
Threat Intelligence Exchange verifies the reputation of executable programs on the endpoints connected to these files.

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

When the Threat Intelligence Exchange server is detected, Threat Intelligence Exchange watchlists, data enrichment, and correlation rules are added automatically and Threat Intelligence Exchange alarms are enabled. You receive a visual notification, which includes a link to the summary of the changes made. You are also notified if the Threat Intelligence Exchange server is added to the McAfee ePO server after the device has been added to the ESM.

Once Threat Intelligence Exchange events are generated, you can view their execution history (see View Threat Intelligence Exchange execution history and set up actions) and select the actions you want to take on the malicious data.

**Correlation rules**
Six correlation rules are optimized for Threat Intelligence Exchange data. They generate events that you can search and sort through.
• TIE — GTI reputation changed from clean to dirty
• TIE — Malicious file (SHA-1) found on increasing number of hosts
• TIE — Malicious file name found on increasing number of hosts
• TIE — Multiple malicious files found on single host
• TIE — TIE reputation changed from clean to dirty
• TIE — Increase in malicious files found across all hosts

Alarms
The ESM has two alarms that might trigger when important Threat Intelligence Exchange events are detected.

• TIE bad file threshold exceeded triggers from the correlation rule TIE - Malicious file (SHA-1) found on increasing number of hosts.

• TIE unknown file executed triggers from a specific TIE event and adds information to the TIE data source IPs watchlist.

Watchlist
The TIE data source IPs watchlist maintains a list of systems that have triggered the TIE unknown file executed alarm. It is a static watchlist with no expiration.

Threat Intelligence Exchange execution history
You can view the execution history for any Threat Intelligence Exchange event (see View Threat Intelligence Exchange execution history and set up actions), which includes a list of the IP addresses that have attempted to execute the file. On this page, you can select an item and take any of these actions:

• Create a new watchlist.
• Add the information to a blacklist.
• Append the information to a watchlist.
• Export the information to a .csv file.
• Create a new alarm.

View Threat Intelligence Exchange execution history and set up actions
The Threat Intelligence Exchange execution history page displays a list of systems that have executed the file associated with the event you selected.

Before you begin
An ePolicy Orchestrator device with an attached Threat Intelligence Exchange server on the ESM must exist.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree of the ESM console, click the ePolicy Orchestrator device.

2. On the views drop-down list, select Event Views | Event Analysis, then click the event.

3. Click the menu icon, then select Actions | TIE Execution History.
On the TIE Execution History page, view the systems that have executed the Threat Intelligence Exchange file.

To add this data to your workflow, click a system, click the Actions drop-down menu, then select an option to open its ESM page.

Set up the action you selected (see the online Help for instructions).

**Query McAfee ePO devices for a report or view**
You can query multiple McAfee ePO devices for a report or view if they are integrated with McAfee Real Time for McAfee ePO.

**Before you begin**
Verify that McAfee ePO devices to be queried are integrated with McAfee Real Time for McAfee ePO.

**Task**  
For option definitions, click ? in the interface.

1. On the system navigation tree, click the system, click the Properties icon, then click Reports.
2. Click Add, fill out sections 1 through 4, then click Add in section 5.
3. On the Report Layout editor, drag and drop a Table, Bar Chart, or Pie Chart component.
4. On the Query Wizard, select Real Time for McAfee EPO on the drop-down list, then select the element or question for the query.
5. Click Next, click Devices, then select the McAfee ePO devices to be queried.
6. (Optional) Click Filters, add filter values for the query, then click OK.
7. If you selected Custom ePO Question on the drop-down list, click Fields, select the elements that you want to include in the question, then click OK.
8. Click Finish to close the Query Wizard, define the properties in the Properties pane, then save the report.

**Query McAfee ePO devices for data enrichment**
You can query multiple McAfee ePO devices for data enrichment if they are integrated with McAfee Real Time for McAfee ePO.

**Before you begin**
Verify that McAfee ePO devices to be queried are integrated with McAfee Real Time for McAfee ePO.

**Task**  
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, click the Properties icon, then click Data Enrichment.
2. Click Add, type a name, then make the selections on the Main tab.
3 On the **Source** tab, select McAfee Real Time for McAfee ePO in the **Type** field, then select the devices in the **Device** field.

4 Set the remaining settings on the **Query**, **Scoring**, and **Destination** tabs, then click **Finish**.

**Query McAfee ePO devices for McAfee Real Time for McAfee ePO dashboard**

You can run a query of multiple McAfee ePO devices on the McAfee Real Time for McAfee ePO dashboard view.

**Before you begin**

Verify that McAfee ePO devices to be queried are integrated with McAfee Real Time for McAfee ePO.

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, click the McAfee ePO devices to be queried.

2 On the ESM console, click the views list, then select McAfee Real Time for McAfee ePO.

3 Select the filters in the **Filters** pane:
   a In the **Elements** section, click the open field and select the elements for the query.
   b In the **Filters** section, select the type of filter, then type the filter in the open field.
   c Select the filter action, then type the value.

4 Click the **Run Query** icon ✂️.

**Nitro Intrusion Prevention System (Nitro IPS) settings**

The McAfee Nitro Intrusion Prevention System (Nitro IPS) device detects sophisticated network intrusion attempts and actively records and thwarts these attempts. The Nitro IPS device includes an embedded data manager (used for administration, data acquisition, and analysis) and advanced intrusion analytics such as anomaly detection.

The device selectively passes, drops, and logs packets as they arrive, based on a user-defined rule set specified by an industry-standard rule language. Each Nitro IPS device contains a fully functional firewall component controlled by industry-standard firewall rules providing low-level packet inspection capabilities and an industry-standard system log.

**Anomaly Detection Wizard**

Anomaly detection is accessible for any Nitro IPS or virtual device but is only useful for those that have been gathering flow data. The **Rate-Based Anomaly Detection Wizard** shows a list and description of all the variables available on the selected device.

Certain firewall rules are rate-based. A rate-based rule is a rule that triggers an alert only if your network traffic exceeds the thresholds defined by firewall-category variables in the **Policy Editor**. The default values for these variables might not make sense for your network’s traffic, so the **Rate-Based Anomaly Detection Wizard** provides the ability to analyze graphs of your network flow data as it relates to these parameters. You can then select the default values, specify your own value, or choose to have the ESM analyze your data and try to make some best guesses as to what these values should be based on the history of your network’s traffic. Every network is different, so we recommend that you familiarize yourself with your traffic history by reviewing these visual analysis reports and choosing values that fit your needs.
The wizard performs many complicated computations to calculate suggested values for the rate-based anomaly parameters and to present you with a visual analysis of your network traffic patterns. If your Nitro IPS, virtual device, Receiver, and data source have a large amount of flow data, it is suggested that you limit the time range used in these calculations. Use a few days or a week of normal network activity as a baseline for calculating these values. Using a longer time period may cause these calculations to take longer than desired.

Here is a list of the rate-based anomaly firewall rules and the variables that affect their operation:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large inbound byte rate</td>
<td>LARGE_INBOUND_BYTE_RATE_LIMIT, LARGE_INBOUND_BYTE_RATE_SECS</td>
</tr>
<tr>
<td>Large inbound bytes</td>
<td>LARGE_INBOUND_BYTES_LIMIT</td>
</tr>
<tr>
<td>Large inbound network connections rate</td>
<td>LARGE_IB_CONN_RATE_BURST, LARGE_IB_CONN_RATE_LIMIT</td>
</tr>
<tr>
<td>Large inbound packet rate</td>
<td>LARGE_INBOUND_PACKET_RATE_LIMIT, LARGE_INBOUND_PACKET_RATE_SECS</td>
</tr>
<tr>
<td>Large inbound packet</td>
<td>LARGE_INBOUND_PACKETS_LIMIT</td>
</tr>
<tr>
<td>Large outbound byte rate</td>
<td>LARGE_OUTBOUND_BYTE_RATE_LIMIT, LARGE_OUTBOUND_BYTE_RATE_SECS</td>
</tr>
<tr>
<td>Large outbound network connection rate</td>
<td>LARGE_OB_CONN_RATE_BURST, LARGE_OB_CONN_RATE_LIMIT</td>
</tr>
<tr>
<td>Large outbound packet rate</td>
<td>LARGE_OUTBOUND_PACKET_RATE_LIMIT, LARGE_OUTBOUND_PACKET_RATE_SECS</td>
</tr>
<tr>
<td>Large outbound packets</td>
<td>LARGE_OUTBOUND_PACKETS_LIMIT</td>
</tr>
<tr>
<td>Long connection duration</td>
<td>LONG_DURATION_SECONDS</td>
</tr>
</tbody>
</table>

**Edit anomaly detection variables**

The Rate-based Anomaly Detection Wizard lists the anomaly detection variables and provides several options you can use to analyze the rate-based anomaly detection data.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a Nitro IPS or virtual device that gathers flow data, then click the Properties icon.
2. Click Edit in the Anomaly Detection Wizard field.
3. Perform any of the available functions, then click OK.

**Generate an Analysis Report**

The Analysis Report provides a visual analysis of various aspects of your network traffic. This report is useful for getting a feel of your network traffic patterns through visual inspection. The data you gather can help you make decisions when choosing values for the rate-based anomaly rule parameters.

> To generate a report, the device must have at least 10,000 flows generated.
Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select a Nitro IPS that has been gathering flow data, then click the Properties icon.

2 Click Edit in the Anomaly Detection Wizard field.

3 Click Analysis | Analysis Report, then select the time range and variable for the report.

4 Click OK.

The report is generated. The vertical and horizontal scales can be zoomed in and out by clicking and dragging the circular icons on the chart axes, if available.

Access firewall and standard rules
Rules are added and maintained on the Policy Editor. However, you can read, write, view, export, and import firewall and standard rules from the IPS or IPS virtual devices.

Rules should not be regularly maintained from this page. Changing the rules in this way causes the device policy settings to be out-of-sync with the settings in the Policy Editor.

Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select IPS Properties, then click Firewall Rules or Standard Rules.

2 Select any of the options, then click OK.

IPS or virtual device blacklist
The blacklist blocks traffic as it flows through the device before it is analyzed by the deep packet inspection engine.

Using the Blacklist Editor, you can manually manage blocked sources, blocked destinations, and exclusion settings for the device. You can also select whether you want this device to be subjected to the Global Blacklist settings. The Include Global Blacklist checkbox at the top of the editor must be selected if you want this device to include these settings.

The Blacklist Editor screen includes three tabs:

- Blocked Sources — Matches against the source IP address of traffic passing through the device.
- Blocked Destinations — Matches against the destination IP address of traffic passing through the device.
- Exclusions — Provides immunity from being automatically added to either of the blacklists. Critical IP addresses (for example, DNS and other servers or system administrators' workstations) can be added to the exclusions to make sure that they are never automatically blacklisted, regardless of what events they might generate.

Entries in both the Blocked Sources and the Blocked Destinations tab can be configured to narrow the effect of the blacklist to a specific destination port.

Hosts can also be added to or removed from the blacklist manually. When one of the tabs in the Blacklist Editor is selected, you can add or modify an entry. Fields required to add an entry include IP Address, Port (versions 6.2.x and later), and Duration (permanent or temporary). There is also an optional Description field.
Keep this in mind when adding entries:

- **Add** and **Modify** are enabled based on the information you change. When you change the IP address or port, **Add** is enabled. If you change the duration or description, **Modify** is enabled.

- Entries in the **Blocked Sources** and **Blocked Destination** lists can be configured to blacklist on all ports or a specific port.

- Entries that use a masked range of IP addresses must be configured with the port set to **any** (0) and the duration must be permanent.

- Entries can be added temporarily (specified in minutes, hours, or days) or permanently. However, entries in the **Exclusions** must be permanent.

- While these lists require IP address format, a tool is included to help add meaning to these addresses. After entering an IP address or host name in the **IP Address** field, the button next to that control says **Resolve** or **Lookup**, based on the value entered. Selecting **Resolve** resolves the entered host name and populates the **IP Address** field with that information, and moves the host name to the **Description** field. Selecting **Lookup** performs a lookup on the IP address and populates the **Description** field with the results of that lookup. Some websites have more than one IP address, or have IP addresses that are not always the same, so don't rely on this tool to ensure blocking of some websites.

You can select IP addresses on the list and view events they generated on a summary report. This allows you to see the events the offenders triggered, events that were added to the blacklist, or other attacks they might have instigated before being blacklisted.

The **Blacklist Editor** also allows you to apply, reload, and remove events.

### Manage the IPS blacklist

You can manage the IPS blacklist on the **Blacklist Editor**. You can add, modify, or delete items, write changes to the blacklist, read new and updated information from the device, view events generated by the offending IP addresses, and lookup or resolve a host name or IP address.

#### Task

For option definitions, click ? in the interface.

1. On the system navigation tree, select **IPS Properties**, then click **Blacklist | Editor**.

2. Select the **Blocked Sources**, **Blocked Destinations**, or **Exclusions** tab.

3. Perform the actions you want, then click **Close**.

### Configure auto-blacklist

The **Auto-Blacklist Settings** page allows you to manage auto-blacklist configuration settings for the device.

- **Auto-blacklist configuration is performed on a per-device basis.**

#### Task

For option definitions, click ? in the interface.

1. On the system navigation tree, select **IPS Properties**, then click **Blacklist | Settings**.

2. Define the settings as needed, then click **OK**.
McAfee Vulnerability Manager settings

The McAfee Vulnerability Manager can be added to the ESM as a device, allowing you to start a scan on the McAfee Vulnerability Manager from the ESM. This is useful if you purchased a McAfee Vulnerability Manager device and want to run it from the ESM.

McAfee Vulnerability Manager must be associated with a Receiver because the events are pulled from the Receiver, not the McAfee Vulnerability Manager.

Obtain McAfee Vulnerability Manager certificate and passphrase

You must obtain the McAfee Vulnerability Manager certificate and passphrase before setting up McAfee Vulnerability Manager connections. This task is not performed on the ESM.

**Task**
For option definitions, click ? in the interface.

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

The Scans page shows all the vulnerability scans that are running or have run from McAfee Vulnerability Manager, and their status. When you open this page, an API checks if there are default web login credentials. If there are, the scan list is populated based on those credentials, and is updated every 60 seconds. You can initiate a new scan from this page as well.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select MVM Properties, then click Scans.
2. Click New Scan and enter the information requested.
3. Click OK.

When the scan is complete it's added to the list of scans.

Set up McAfee Vulnerability Manager connection

You must set up McAfee Vulnerability Manager connections to the database to pull the vulnerability assessment data from McAfee Vulnerability Manager, and to the web user interface to perform scans on McAfee Vulnerability Manager.

**Before you begin**
You must obtain the McAfee Vulnerability Manager certificate and passphrase

Changing these settings doesn't affect the device itself. It only affects the way the device communicates with the ESM.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select MVM Properties, then click Connection.
2. Fill in the information requested, then click OK.

**McAfee Network Security Manager settings**
The McAfee Network Security Manager can be added to the ESM as a device, allowing you to access the functions from the ESM. This is useful if you purchased a device and want to access it from the ESM.

When you add a McAfee Network Security Manager device to the ESM, the sensors on the device are listed as children under the device on the system navigation tree. The device must be associated with a Receiver because the events are pulled from the Receiver, not the McAfee Network Security Manager.

**Add a blacklist entry**
The McAfee Network Security Manager applies blacklisting through the sensors. The Blacklist page displays the blacklist entries that were defined for the sensor that you select. From this page, you can add, edit, and delete blacklist items.

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select NSM Properties, click Blacklist, then select a sensor.
2. To apply the global blacklist entries to this sensor, select Include Global Blacklist.
   
   The global blacklist item is added to the list. If there are duplicate IP addresses, the global blacklist address overwrites the McAfee Network Security Manager address.

   > Once you select this option, it can’t be undone automatically. You must delete items manually.

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

   The entry appears on the blacklist until its duration expires.

**Add or delete a removed blacklist entry**
Any entry that was initiated on the ESM with a duration that hasn’t expired, but is not returned on the list of blacklist entries when the McAfee Network Security Manager (Manager) is queried, is displayed with a Removed status and a flag icon.

This condition occurs if the entry was removed, but the removal was not initiated on the ESM. You can re-add this entry to or delete it from the blacklist.

**Task**
For option definitions, click ? in the interface.

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.
Configuring ancillary services

Ancillary services include Remedy servers, Network Time Protocol (NTP) servers, and DNS servers. Configure these servers to communicate with ESM.

Contents

- General system information
- Configure Remedy server settings
- Defining message settings
- Set up NTP on a device
- Configure network settings
- System time synchronization
- Install a new certificate
- Configure profiles
- SNMP configuration

General system information

On the System Properties | System Information page, you can see general information about your system and the status of various functions. On the System Log page, you can see events that have taken place on the system or devices.

You can refer to this information when you speak with McAfee support about your system, when you are setting up features such as event or flow aggregation, or to check on the status of a rules update or system backup.

- **System**, **Customer ID**, **Hardware**, and **Serial Number** provide information about the system and its current operational status.

- **Database Status** shows when the database is performing other functions (for example, a database rebuild or background rebuild) and the status of those functions. An OK status means that the database is operating normally.

- **System Clock** shows the date and time that System Properties was last opened or refreshed.

- **Rules Update; Events, Flows & Logs** and **Backup & Restore** show the last time the rules were updated; events, flows, and logs were retrieved; and a backup and restore was performed.

- When in FIPS mode, **FIPS self-test** and **Status** show the last time a FIPS self-test was performed and its status.

- **View Reports** shows the ESM Device Type Count and Event Time reports.

Configure Remedy server settings

If you have a Remedy system set up, you must configure the remedy settings so the ESM can communicate with it.

**Before you begin**

Set up your Remedy system.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Custom Settings | Remedy.

2. On the Remedy Configuration page, enter the information for your Remedy system, then click OK.
When you select Send event to Remedy on the Event Analysis view, the email is populated with the information that you entered on this page.

**Defining message settings**

When you define the action settings for an alarm or set up the delivery method for a report, you can choose to send a message. To do this, you must connect the ESM to your mail server and configure the recipients you want to send email, SMS, SNMP, or syslog messages to.

Alarm notifications can be sent using the SNMP v1 protocol. SNMP uses User Datagram Protocol (UDP) as the transport protocol for passing data between managers and agents. In a typical SNMP setup, an agent such as the ESM, can forward events to an SNMP server (usually referred to as a Network Management Station [NMS]) using packets of data known as traps. This can be useful when you want to receive event reports from the ESM in the same way notifications are received from other agents in the network. Due to size limitations of the SNMP trap packets, each line of the report is sent in a separate trap.

Query CSV reports generated by the ESM can also be sent using syslog. The query CSV reports are sent one line per syslog message, with the data of each line of the query results arranged in comma-separated fields.

**Connect your mail server**

Configure the settings to connect to your mail server so you can send alarm and report messages.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, click Email Settings, and enter the host and port for your email server.

2. Provide the information requested to connect to your mail server.

3. Click Apply or OK to save the settings.

**See also**

Manage recipients on page 154

**Manage recipients**

Alarm or report messages can be sent in several formats, each of which has a list of recipients that you can manage. Email addresses can be grouped so you can send a message to several recipients at once.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Email Settings.

2. Click Configure Recipients, then select the tab you want to add them to.

3. Click Add, then add the requested information.

4. Click OK.

The recipient is added to the ESM and you can select them anywhere recipients are used throughout the ESM.
Set up NTP on a device
Synchronize the device time with the ESM using a Network Time Protocol (NTP) server.

Task
For option definitions, click ? in the interface.

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.

Tasks
- View status of NTP servers on page 155
  View the status of all the NTP servers on the ESM.

View status of NTP servers
View the status of all the NTP servers on the ESM.

Before you begin
Add NTP servers to the ESM or devices (see System time synchronization or Set up NTP on a device).

Task
For option definitions, click ? in the interface.

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.

See also
System time synchronization on page 161
Set up NTP on a device on page 38

Configure network settings
Configure the way ESM connects to your network by adding ESM server gateway and DNS server IP addresses, defining proxy server settings, setting up SSH, and adding static routes.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Network Settings.
2. Fill in the information to configure the connection to your network.
3. Click Apply or OK.
Tasks

- **Set up the IPMI port on ESM or devices on page 158**
  Configure the network for the IPMI port to set up IPMI on the ESM or its devices.

- **Set up network traffic control on the ESM on page 159**
  Define a maximum data output value for the ESM.

- **Set up DHCP on page 160**
  Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

- **Set up DHCP on VLAN on page 160**
  Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

Managing network interfaces

Communication with a device can take place using the public and private interfaces of the traffic paths. This means that the device is invisible in the network because it doesn't require an IP address.

Management interface

Alternately, network administrators can configure a management interface with an IP address for communication between the ESM and the device. These features of a device require the use of a management interface:

- Full control of bypass network cards
- Use of NTP time synchronization
- Device-generated syslog
- SNMP notifications

Devices are equipped with at least one management interface, which gives the device an IP address. With an IP address, the device can be accessed directly by the ESM 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.

For a device running in Nitro IPS mode, there must be two interfaces for each path of network traffic. For IDS mode, there must be a minimum of two network interfaces in the device. You can configure more than one management network interface in the device.

Bypass NIC

A device in bypass mode allows all traffic to pass, including malicious traffic. Under normal circumstances, you can have a one- to three-second loss of connection when the device switches to bypass mode, and an 18-second loss when it switches out. Being connected to certain switches, such as some models of Cisco Catalyst, can change these numbers. In this case, you can have a 33-second loss of connection when the device switches to bypass mode and when it switches out.

If you have the scenario where it takes 33 seconds to reestablish communications, you can enable port fast on the switch port and manually set the speed and duplex to get the times back to normal. Be sure to set all four ports (switch, both on Nitro IPS, and other device) to the same setting or you might have a negotiation problem in bypass mode (see Set up bypass NICs).

The available bypass options depend on the type of bypass NIC in the device, Type 2 or Type 3.
Set up network interfaces
Interface settings determine how the ESM connects to the device. You must define these for each device.

Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select a device, then click the Properties icon.
2 Click the device’s Configuration option, then click Interfaces.
3 Enter the data as requested, then click Apply.

All changes are pushed to the device and take effect immediately. Upon applying changes, the device re-initializes, causing all current sessions to be lost.

Add VLANs and aliases
Add Virtual Local Area Networks (VLANs) and aliases (assigned IP address and netmask pairs that you add if you have a network device that has more than one IP address) to an ACE or ELM interface.

Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select a device, then click the Properties icon.
2 Click device Configuration, click Interfaces, then click Advanced.
3 Click Add VLAN, enter the information requested, then click OK.
4 Select the VLAN you want to add the alias to, then click Add Alias.
5 Enter the information requested, then click OK.

Add static routes
A static route is a set of instructions about how to reach a host or network that is not available through the default gateway.

Task
For option definitions, click ? in the interface.

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.

Bypass NIC
Under normal circumstances, you can have a one- to three-second loss of connection when the device switches to bypass mode, and an 18-second loss when it switches out. Being connected to certain switches, such as some models of Cisco Catalyst, can change these numbers. In this case, you can have a 33-second loss of connection when the device switches to bypass mode and when it switches out.
If you have the scenario where it takes 33 seconds to reestablish communications, you can enable port fast on the switch port and manually set the speed and duplex to get the times back to normal. Be sure to set all four ports (switch, both on Nitro IPS, and other device) to the same setting or you might have a negotiation problem in bypass mode.

The available bypass options depend on the type of bypass NIC in the device, Type 2 or Type 3.

**Set up bypass NICs**

On IPS devices, you can define bypass NIC settings to allow all traffic to pass through.

```
ADM and DEM devices are always in IDS mode. You can view their bypass NIC type and status but you can't change their settings.
```

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Configuration | Interfaces.
3. On the Network Interface Settings page, go to the Bypass NIC Configuration section at the bottom.
4. View the type and status or, on an IPS, change the settings.
5. Click OK.

**IPMI port set up on ESM or devices**

You can set up the IPMI port on the ESM or any of its devices. This enables you to perform several actions:

- Plug the IPMI Network interface controller (NIC) into a switch so that it is available to IPMI software.
- Set the IPMI password for the default user after upgrade to ESM 9.4.0.
- Access IPMI commands like power-on and power status.
- Reset the IPMI card.
- Perform a warm and cold reset.

**Set up the IPMI port on ESM or devices**

Configure the network for the IPMI port to set up IPMI on the ESM or its devices.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the system or any of the devices, then click the Properties icon.
2. Access the Network Settings Advanced tab.
   - On the ESM, click Network Settings | Advanced.
   - On a device, click the Configuration option for the device, then click Interfaces | Advanced.
3 Select **Enable IPMI Settings**, then type the VLAN, IP address, netmask, and gateway for the IPMI.

> If **Enable IPMI Settings** is grayed out on device BIOS, you need to update the system BIOS. SSH to the device and open the /etc/areca/system_bios_update/Contents-README.txt file.

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

> If you are upgrading your device, you might receive a message telling you to change the password or re-key the device. If you receive this message, change the system password or re-key the device to set a new password to configure the IPMI.

### Set up network traffic control on the ESM

Define a maximum data output value for the ESM.

This feature is helpful when you have bandwidth restrictions and need to control the amount of data that can be sent out by each ESM. The options are kilobits (Kb), megabits (Mb), and gigabits (Gb) per second.

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

**Task**

For option definitions, click ? in the interface.

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

2. Click **Network Settings**, then click the **Traffic** tab.

   The table lists the existing controls.

3. To add controls for a device, click **Add**, enter the network address and mask, set the rate, then click **OK**.

   > If you set the mask to zero (0), all the data sent is controlled.

4. Click **Apply**.

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

### Working with host names

The host name of a device is usually more useful than the IP address. You can manage host names so that they are associated with their corresponding IP address.

On the **Hosts** page, you can add, edit, remove, lookup, update, and import host names, as well as set the time after which an auto-learned host name expires.

When you view event data, you can show the host names associated with the IP addresses in the event by clicking the **Show host names** icon located at the bottom of view components. If existing events are not tagged with a host name, the system searches the host table on the ESM and tags the IP addresses with their host names. If the IP addresses are not listed on the host table, the system performs a Domain Name System (DNS) lookup to locate the host names. The search results then show up in the view and are added to the host table. On the host table, this data is marked as **Auto Learned** and expires after the period of time designated in the **Entries expire after** field located below the host table on the **System Properties | Hosts** page. If the data has expired, another DNS lookup is performed the next time you select the **Show host names** option 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 a host name and IP address individually or by importing a tab-delimited list of host names and IP addresses. The more data you enter in this manner, the less time is spent on DNS look ups. If you enter a host name manually, it doesn't expire, but you can edit or remove it.

**Manage host names**

Perform all the actions necessary to manage host names on the Hosts page such as adding, editing, importing, removing, or looking them up. You can also set the expiration time for auto-learned hosts.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Hosts.
2. Select an option and enter the information requested.
3. Click Apply or OK.

**Set up DHCP**

Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

When you set up the ESM to deploy in the cloud environment, DHCP is enabled automatically and assigns an IP address. When not in the cloud environment, you can enable and disable DHCP services on the ESM, non-HA Receiver, ACE, and ELM if you have Device Management rights. This would be useful if you need to reset the IP addresses for your network.

Aliases are disabled when DHCP is enabled.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the system or a device, then click the Properties icon.
2. Do one of the following:
   - For the ESM, click Network Settings, then click the Main tab.
   - For a device, select the device's Configuration option, click Interfaces, then click the Network tab.
3. Click Setup for the Interface 1 field, then select DHCP.
   
   For devices other than Receivers, you are informed that the changes require an ESM server restart.
4. Click OK.

**Set up DHCP on VLAN**

Dynamic Host Configuration Protocol (DHCP) is used on IP networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

When you set up the ESM to deploy in the cloud environment, DHCP is enabled automatically and assigns an IP address. When not in the cloud environment, you can enable and disable DHCP services on the VLANs, ESM, non-HA Receiver, ACE, and ELM if you have Device Management rights. This would be useful if you need to reset the IP addresses for your network.
Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system or a device, then click the Properties icon.

2. Do one of the following:
   - For the ESM, click Network Settings, then click the Main tab.
   - For a device, select the device's Configuration option, click Interfaces, then click the Network tab.

3. Click Setup for the Interface 1 field, then click Advanced.

4. Click Add VLAN, type the VLAN, then select DHCP.

5. Click OK to return to the Network Settings page, then click Apply.

For devices other than Receivers, you are informed that the changes require an ESM server restart.

System time synchronization
Since activities generated by the ESM and its devices are time stamped, it is important that the ESM and devices be synchronized to keep a constant frame of reference for data they gather. You can set the ESM system time or select to have the ESM and devices synchronized to an NTP server.

Set up system time

Before you begin
If you want to add NTP servers to the ESM, set up the NTP servers and have their authorization keys and key IDs.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties and ensure System Information is selected.

2. Click System Clock (GMT), define the settings, then click OK.

   NTP server addresses on IPS class devices must be IP addresses.

The server information is saved in the configuration file. You can then access the list of NTP servers again and check their status.

Sync device clocks
You can sync the device clocks with the ESM clock so that the data generated by the various systems reflects the same time setting.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties or device Properties, then click Sync in the Sync Device Clock field.

   You are informed when the sync is complete or if there is a problem.

2. Click Refresh to update the data on the System Information or device Information page.
Install a new certificate
The ESM ships with a default self-signed security certificate for esm.mcafee.local. Most web browsers display a warning that the certificate's authenticity can't be verified. Once you obtain the SSL key certificate pair that you want to use for your ESM, you must install it.

Task
For option definitions, click ? in the interface.
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.

Configure profiles
Define profiles for syslog-based traffic so you can perform setups that share common information without entering the details each time. You can also add a remote command profile (URL or Script) and use it on a view or an alarm.

Task
For option definitions, click ? in the interface.
1. On the system navigation tree, select System Properties, then click Profile Management.
2. To add a profile, click Add on the System Profiles tab, then fill in the profile data.
3. To add a remote command, click the Remote Command tab, then fill in the requested information.
4. Click OK.

SNMP configuration
Configure the settings used by the ESM to send link up and down and cold and warm start traps, both from the ESM and each device; retrieve Management Information Base (MIB)-II system and interface tables; and allow discovery of the ESM through an SNMP walk.

SNMPv3 is supported with NoAuthNoPriv, AuthNoPriv, and AuthPriv options, using MD5 or Secure Hash Algorithm (SHA) for authentication and Data Encryption Standard (DES) or Advanced Encryption Standard (AES) for encryption (MD5 and DES are not available in FIPS compliance mode).

SNMP requests can be made to an ESM for ESM, Receiver, and Nitro IPS health information, and SNMPv3 traps can be sent to an ESM to add to the blacklist of one or more of its managed Nitro IPS devices. All McAfee appliances can also be configured to send link up and down traps and warm and cold boot traps to one or more destinations of your choosing (see SNMP and the McAfee MIB).

Configure SNMP settings
Define the settings used by the ESM for inbound and outbound SNMP traffic. SNMP queries can only be performed by users whose user names don't include a space.

Task
For option definitions, click ? in the interface.
1. On the system navigation tree, select System Properties, then click SNMP Configuration.
2. Enter the required information on the SNMP Requests and SNMP Traps tabs.
3. Click OK.
Set up SNMP trap for power failure notification
Select an SNMP trap to notify you of general hardware failures and DAS power failures, to keep the system from shutting down due to a power failure.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, then click the Properties icon.
2. Click SNMP Configuration, click the SNMP Traps tab, then select General Hardware Failure.
3. Click Apply or OK.

When a power supplies fails, an SNMP trap is sent and a health status flag appears next to the device on the system navigation tree.
You can add an alarm to trigger when a failure occurs (see Add a power failure notification alarm).

Create an SNMP trap as an action in an alarm
You can send SNMP traps as an action within an alarm.

Before you begin
Prepare the SNMP trap Receiver (only required if you don't have an SNMP trap Receiver).

For option definitions, click ? in the interface.

Task
1. Create an SNMP profile to tell the ESM where to send the SNMP traps.
   a. On the system navigation tree, select the system then click the Properties icon.
   b. Click Profile Management, then select SNMP Trap in the Profile Type field.
   c. Fill in the remaining fields, then click Apply.
2. Configure SNMP on the ESM.
   a. On System Properties, click SNMP Configuration, then click the SNMP Traps tab.
   b. Select the port, select the types of traps to send, then select the profile you added in Step 1.
   c. Click Apply.
3. Define an alarm with SNMP Trap as an action.
   a. On System Properties, click Alarms, then click Add.
   b. Fill in the information requested on the Summary, Condition, and Devices tabs, selecting Internal Event Match as the condition type, then click the Actions tab.
   c. Select Send Message, then click Configure to select or create a template for SNMP messages.
   d. Select Basic SNMPTrap in the SNMP field, or click Templates, then click Add.
   e. Select an existing template or click Add to define a new template.
   f. Return to the Alarm Settings page, then proceed with alarm setup.
Add a power failure notification alarm

Add an alarm to notify you when either of the ESM power supplies fail.

**Before you begin**

Set up a General Hardware Failure SNMP trap (see Set up SNMP trap for power failure notification).

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, then click the Properties icon.
2. Click Alarms, click Add, add the requested data on the Summary tab, then click the Condition tab.
3. In the Type field, select Internal Event Match.
4. In the Field field, select Signature ID, then type 306-50086 in the Value(s) field.
5. Fill in the remaining information on each tab as needed, then click Finish.

An alarm triggers when a power supply fails.

**SNMP and the McAfee MIB**

Several aspects of the McAfee product line can be accessed through SNMP. The McAfee MIB defines the object identifiers (OIDs) for each object or characteristic of interest.

The MIB defines object groups for:

- **Alerts** — An ESM can generate and send alert traps using Event Forwarding. A Receiver can receive alert traps by configuring a McAfee SNMP data source.
- **Flows** — A Receiver can receive flow traps by configuring a McAfee SNMP data source.
- **ESM Health Requests** — An ESM can receive and respond to health requests for itself and the devices it manages.
- **Blacklist** — An ESM can receive traps defining entries for blacklists and quarantine lists, which it then applies to the Nitro IPS devices 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 SNMPv2 Structure of Management Information (SMI)-compliant. McAfee products that use SNMP can be configured to work over SNMPv1, SNMPv2c, and SNMPv3, including authentication and access control.

Health requests are made by using the SNMP GET operation. The SNMP GET operation is used by SNMP manager applications to retrieve values from the managed objects maintained by the SNMP agent (in this case, the ESM). The applications typically perform an SNMP GET request by providing the host name of the ESM and OIDs, along with the specific instance of the OID.

The ESM responds with a return value or with an error. For example, a health request and response for the health of the Nitro IPS with Nitro IPS ID 2 might look like this:
<table>
<thead>
<tr>
<th>Request and response OID</th>
<th>Units</th>
<th>Response value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.1.2</td>
<td>Internal Nitro IPS</td>
<td>Nitro IPS name</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.2.2</td>
<td>2</td>
<td>ESM unique identifier of the Nitro IPS</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.3.2</td>
<td>1</td>
<td>Communication with the Nitro IPS is available (1) or not available (0)&quot;</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.4.2</td>
<td>Ok</td>
<td>Status of the Nitro IPS</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.5.2</td>
<td>off</td>
<td>Status of the Nitro IPS's bypass NICs</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.6.2</td>
<td>Nitro IPS</td>
<td>Nitro IPS mode (Nitro IPS or IDS)</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.7.2</td>
<td>percent</td>
<td>2</td>
<td>Percentage combined instantaneous CPU load</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.8.2</td>
<td>MB</td>
<td>1010</td>
<td>Nitro IPS RAM total</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.9.2</td>
<td>MB</td>
<td>62</td>
<td>Available RAM</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.10.2</td>
<td>MB</td>
<td>27648</td>
<td>Total HDD space partitioned for Nitro IPS database</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.11.2</td>
<td>MB</td>
<td>17408</td>
<td>Free HDD space available for Nitro IPS database</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.12.2</td>
<td>seconds since 1970-1-1 00:00:00.0 (GMT)</td>
<td>120793661</td>
<td>Current system time on the Nitro IPS</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.13.2</td>
<td>7.1.3 20070518091421a</td>
<td></td>
<td>Nitro IPS version information and buildstamp</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.14.2</td>
<td>ABCD:1234</td>
<td>Nitro IPS machine ID</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.15.2</td>
<td>Nitro IPS</td>
<td>Nitro IPS model number</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.16.2</td>
<td>alerts per minute</td>
<td>140</td>
<td>Alert rate (per minute) for last 10 minutes</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.2.17.2</td>
<td>flows per minute</td>
<td>165</td>
<td>Flow rate (per minute) for last 10 minutes</td>
</tr>
</tbody>
</table>

Using the example above, the SNMP manager makes a request to the SNMP agent, the ESM. The numbers mean:

- 1.3.6.1.4.1.23128 — The McAfee Internet Assigned Numbers Authority (IANA)-assigned enterprise number
- 1.3.2 — A Nitro IPS health request
- The second to last number (1–17 above) — For requesting the various aspects of Nitro IPS health
- The final number (2) — The specific instance of the OID, the Nitro IPS ID

The ESM responds by populating the OID bindings with the results of the health request.
The following tables show the meaning of the ESM and Receiver OIDs.

**Table 3-37  ESM health**

<table>
<thead>
<tr>
<th>Request and response OID</th>
<th>Units</th>
<th>Response value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.1</td>
<td>percent</td>
<td>4</td>
<td>Percentage combined instantaneous CPU load</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.2</td>
<td>MB</td>
<td>3518</td>
<td>Total RAM</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.3</td>
<td>MB</td>
<td>25</td>
<td>Available RAM</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.4</td>
<td>MB</td>
<td>1468006</td>
<td>Total HDD space partitioned for ESM database</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.5</td>
<td>MB</td>
<td>1363148</td>
<td>Free HDD space available for ESM database</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.6</td>
<td>seconds since 1970-1-1 00:00:0.0 (GMT)</td>
<td>1283888714</td>
<td>Current system time on the ESM</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.7</td>
<td>8.4.2</td>
<td></td>
<td>ESM version and buildstamp</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.8</td>
<td>4EEE:6669</td>
<td></td>
<td>Machine ID of the ESM</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.1.9</td>
<td>ESM</td>
<td></td>
<td>ESM model number</td>
</tr>
</tbody>
</table>

**Table 3-38  Receiver health**

<table>
<thead>
<tr>
<th>Request and response OID</th>
<th>Units</th>
<th>Response value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.1</td>
<td>Receiver</td>
<td></td>
<td>Receiver name</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.2</td>
<td></td>
<td>2689599744</td>
<td>ESM unique identifier of the Receiver</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.3</td>
<td></td>
<td>1</td>
<td>Indicates that communication with the Receiver is available (1) or not available (0)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.4</td>
<td>Ok</td>
<td></td>
<td>Indicates the status of the Receiver</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.5</td>
<td>percent</td>
<td>2</td>
<td>Percentage combined instantaneous CPU load</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.6</td>
<td>MB</td>
<td>7155</td>
<td>Total RAM</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.7</td>
<td>MB</td>
<td>5619</td>
<td>Available RAM</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.8</td>
<td>MB</td>
<td>498688</td>
<td>Total HDD space partitioned for Receiver database</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.9</td>
<td>MB</td>
<td>472064</td>
<td>Free HDD space available for Receiver database</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.10</td>
<td>seconds since 1970-1-1 00:00:0.0 (GMT)</td>
<td>1283889234</td>
<td>Current system time on the Receiver</td>
</tr>
</tbody>
</table>
Table 3-38  Receiver health (continued)

<table>
<thead>
<tr>
<th>Request and response OID</th>
<th>Units</th>
<th>Response value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.11</td>
<td></td>
<td>7.1.3 20070518091421a</td>
<td>Receiver version and buildstamp</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.12</td>
<td></td>
<td>SEE:CCC6</td>
<td>Machine ID of the Receiver</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.13</td>
<td></td>
<td>Receiver</td>
<td>Receiver model number</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.14</td>
<td>alerts per minute</td>
<td>1</td>
<td>Alert rate (per minute) for last 10 minutes</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.3.3.15</td>
<td>flows per minute</td>
<td>2</td>
<td>Flow rate (per minute) for last 10 minutes</td>
</tr>
</tbody>
</table>

Events, flows, and blacklist entries are sent using SNMP traps or inform requests. An alert trap sent from an ESM configured to do Event Forwarding might look something like this:

<table>
<thead>
<tr>
<th>OID</th>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.4.1.23128.1.1.1</td>
<td>780</td>
<td>ESM alert ID</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.2</td>
<td>6136598</td>
<td>Device alert ID</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.3</td>
<td>Internal Nitro IPS</td>
<td>Device Name</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.4</td>
<td>2</td>
<td>Device ID</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.5</td>
<td>10.0.0.69</td>
<td>Source IP</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.6</td>
<td>27078</td>
<td>Source Port</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.7</td>
<td>AB:CD:EF:01:23:45</td>
<td>Source MAC</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.8</td>
<td>10.0.0.68</td>
<td>Destination IP</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.9</td>
<td>37258</td>
<td>Destination Port</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.10</td>
<td>01:23:45:AB:CD:EF</td>
<td>Destination MAC</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.11</td>
<td>17</td>
<td>Protocol</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.12</td>
<td>0</td>
<td>VLAN</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.13</td>
<td>1 Flow direction</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.14</td>
<td>20</td>
<td>Event count</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.15</td>
<td>1201791100</td>
<td>First time</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.16</td>
<td>1201794638</td>
<td>Last time</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.17</td>
<td>288448</td>
<td>Last time (microseconds)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.18</td>
<td>2000002</td>
<td>Signature ID</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.19</td>
<td>ANOMALY Inbound High to High</td>
<td>Signature description</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.20</td>
<td>5</td>
<td>Action taken</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.21</td>
<td>1</td>
<td>Severity</td>
</tr>
<tr>
<td>OID</td>
<td>Value</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.22</td>
<td>201</td>
<td>Data source type or result</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.23</td>
<td>0</td>
<td>Normalized signature ID</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.24</td>
<td>0:0:0:0:0:0:0:0</td>
<td>IPv6 source IP</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.25</td>
<td>0:0:0:0:0:0:0:0</td>
<td>IPv6 destination IP</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.26</td>
<td></td>
<td>Application</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.27</td>
<td></td>
<td>Domain</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.28</td>
<td></td>
<td>Host</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.29</td>
<td></td>
<td>User (source)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.30</td>
<td></td>
<td>User (destination)</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.31</td>
<td></td>
<td>Command</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.32</td>
<td></td>
<td>Object</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.33</td>
<td></td>
<td>Sequence Number</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.34</td>
<td></td>
<td>Indicates whether generated in trusted or untrusted environment</td>
</tr>
<tr>
<td>1.3.6.1.4.1.23128.1.1.35</td>
<td></td>
<td>ID of session that generated the alert</td>
</tr>
</tbody>
</table>

The numbers mean:
- 1.3.6.1.4.1.23128 — The McAfee IANA-assigned enterprise number
- 1.1 — A Nitro IPS health request
- The final number (1–35) — For reporting the various characteristics of the alert

For the full details of McAfee MIB definition, see https://x.x.x.x/BrowseReference/NITROSECURITY-BASE-MIB.txt, where x.x.x.x is the IP address of your ESM.

Managing the database

Manage the ESM database to provide information and settings as you set up features on your system.

You can manage database index settings, view and print information about the database memory utilization of events and flows, configure storage locations for inactive partitions, configure the data retention policy for events and flows, and configure how the database allocates space for event and flow data.

If you have more than four CPUs on a VM, you can use the additional storage space for system storage, data storage, and high performance storage.

If you remove more than one drive from the ESM VM at one time, all previous ELM searches can be lost. To avoid this, export the ELM search results before performing this process.
See also
Manage accumulator indexing on page 171
Manage database index settings on page 171
Set up data retention limits on page 170
View database memory utilization on page 172

Set up ESM data storage
There are three types of external storage that can be set up to store ESM data: Internet Small Computer System Interface (iSCSI), Storage Area Network (SAN), and Direct-attached storage (DAS). Once these are connected to the ESM, you can set them up to store data from the ESM.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Database | Data Storage.
2. Click either of the tabs, select an action, then fill in the information requested.
3. Click Cancel to close the page.

See also
Set up data retention limits on page 170

Set up ESM VM data storage
If your ESM VM has more than four CPUs, the VM Data option is available on the Database page, allowing you to use the additional storage you have available for the VM's system storage, data storage, and high performance storage.

Each drop-down list on the Data Allocation page includes the available storage drives that are mounted on the VM.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Database | VM Data.
2. In each field, select the drive you want the data stored on. Each drive can only be selected once.
3. Click OK.

Increase number of available accumulator indexes
Due to the number of enabled standard indexes on the ESM, you can only add five indexes to an accumulator field. If you need more than five, you can disable standard indexes that you are not currently using, such as sessionid, src/dst mac, src/dst port, src/dst zone, src/dst geolocation, up to a maximum of 42.
The ESM uses standard indexes when generating queries, reports, alarms, and views. If you disable any of them, then try to generate a query, report, alarm, or view that uses them, you are notified that it can't be processed because an index is disabled. You are not told which index is affecting the process. Due to this limitation, do not disable standard indexes unless you determine it is absolutely necessary.

1. On the system navigation tree, select **System Properties**, then click **Database**.
2. Click **Settings**, then click the **Accumulator Indexing** tab.
3. From the drop-down list, click **Standard Indexes**, then select **Show standard indexes**.

   The standard indexes are listed in the **Enabled** area.

4. Click the standard indexes to be disabled, then click the arrow to move them to the **Available** area.

   The number in the remaining statement in the top right corner of the page increases with each standard index that you disable.

You can now enable more than five accumulator indexes for the accumulator field that you select (see **Manage accumulator indexing**).

### Set up inactive partitions archive

ESM divides data into partitions. When a partition reaches its maximum size, it becomes inactive and is deleted. You can configure a storage location for inactive partitions so they aren't deleted.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Database** | **Archival**.
2. Fill in the fields, which vary depending on the type you select.
3. Click **OK** to save the settings.

As partitions become inactive, they are copied to this location and are listed on the **Event Partitions** and **Flow Partitions** tabs.

### Set up data retention limits

If you have a configuration that is sending historical data to the system, you can select the length of time that you want events and flows maintained as well as limit the amount of historical data inserted.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Database** | **Data Retention**.
2. Select how long you want events and flows retained and if you want to restrict historical data.
3. Click **OK**.

**See also**

*Set up ESM data storage on page 169*
Define data allocation limits
The maximum number of event and flow records that are maintained by the system is a fixed value. Data allocation allows you to set how much space to allocate for each, and how many records are searched to optimize querying.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Database | Data Allocation.
2. Click the markers on the number lines and drag them to the desired numbers, or click the arrows in the Events and Flows fields.
3. Click OK.

Manage database index settings
Configure options for indexing specific fields of data in the database. If data is not indexed, it's stored but is not displayed in most query results.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Database | Settings.
2. To change the current settings in the Events and Flows columns, click the item you want to change and select a new setting from the drop-down list.
3. If you select Custom in the Port columns, the Port Values screen opens so you can select or add a new port value.
4. Click OK.

Manage accumulator indexing
If you have custom fields that pull numeric data from a source, accumulator indexing can perform sums or averages over time on this data. You can accumulate several events together and average their value or generate a trending value.

**Before you begin**
Set up an accumulator indexing custom type (see Create custom types).

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Database.
2. Click Settings, then click the Accumulator Indexing tab.
3. Select the indexes, then click OK.

You can now set up an accumulator query to display the results.

**See also**
Manage queries on page 250
Create custom types on page 262
View database memory utilization
View and print tables that detail how database memory is being used.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Database | Memory Use.
   The Events and Flows tables list the memory utilization of the database.

2. To print the reports, click the Print icon.

Working with users and groups
Users and groups must be added to the system so that they have access to the ESM, its devices, its policies, and their associated privileges.

When in FIPS mode, ESM has four possible user roles: User, Power User, Key & Certificate Admin, and Audit Admin. When not in FIPS mode, there are two types of user accounts: System Administrator and General User.

The Users and Groups page has two sections:
- Users — Names of users, the number of sessions that each user has open currently, and the groups to which they belong.
- Groups — Names of groups and a description of the privileges assigned to each one.

You can sort the tables by clicking Username, Sessions, or Group Name.

Group privileges
When you set up a group, you set the privileges for the members of the group. If you select Limit access of this group on the Privileges page of Add Group (System Properties | Add Group), access to these features is limited.

- 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.
- 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.
- Reports — Users can only run a report that emails the output to them.
- Watchlists — Users can't add a dynamic watchlist.
- Asset Manager and Policy Editor — Users can't access these features.
- Zones — Users can view only zones they have access to in their list of zones.
- System Properties — Users can access only Reports and Watchlists.
- Filters — Users can't access String Normalization, Active Directory, Assets, Asset Groups, or Tags filter tabs.
- Actions toolbar — Users can't access device management, multi-device management, or Event Streaming Viewer.
Add a user

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties | Users and Groups.
2. Enter the system administrator password, then click OK.
3. In the Users section, click Add, then fill in the information requested.
4. Click OK.

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. An icon appears next to each user name, indicating whether the account is enabled. If the user has administrator privileges, a royalty icon appears next to their name.

Select user settings

The User Settings page gives you the option to change several default settings. You can change the time zone, date format, password, default display, and console language. You can also choose whether to show disabled data sources, the Alarms tab, and the Cases tab.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation bar of the ESM console, click options.
2. Verify that User Settings is selected.
3. Make changes to the settings as needed, then click OK.

The console changes its appearance based on your settings.

Setting up security

Use login security to set up standard login settings, configure the access control list (ACL), and define Common Access Card (CAC) settings. You can also enable Remote Authentication Dial In User Service (RADIUS), Active Directory, and Lightweight Directory Access Protocol (LDAP) authentication (only available if you have system administrator privileges).

ESM security features

The McAfee family of Nitro IPS solutions is designed to be difficult to find on a network and even harder to attack. Nitro IPS devices have no IP stack by default, so packets can’t be addressed directly to the Nitro IPS.

Communication with a Nitro IPS is achieved through the McAfee Secure Encrypted Management (SEM) technology. SEM is an in-band Advanced Encryption Standard (AES) encrypted channel that mitigates the risk of playback or man-in-the-middle types of attacks.

A Nitro IPS device communicates only when addressed by an authorized ESM via the SEM channel. It does not initiate communications on its own. Communication between an ESM and the ESM console is also sent over an AES.
The ESM retrieves authenticated and encrypted signature and software updates from the McAfee central server from an encrypted communication mechanism. Mechanisms, both hardware- and software-based, are in place to make sure devices are managed only from a properly authorized ESM.

**Define standard login settings**
Adjust the settings for standard login procedures by defining how many login attempts can be made in a specified period of time, how long the system can be inactive, password settings, and whether to show the last user ID upon login.

**Task**
For option definitions, click ? in the interface.
1. On the system navigation tree, select **System Properties**, then click **Login Security**.
2. Set the options on the **Standard** tab.
3. Click **OK** or **Apply**.

**Define logon password settings**
There are several settings that you can define for the system logon password.

**Before you begin**
You must have system administrator rights.

**Task**
For option definitions, click ? in the interface.
1. On the system navigation tree, select System Properties, then click Login Security.
2. Click the **Passwords** tab, make your selections, then click **Apply** or **OK**.

**Configure RADIUS authentication settings**
Configure the ESM to authenticate users to a RADIUS server.

**Task**
For option definitions, click ? in the interface.
1. On the system navigation tree, select **System Properties**, then click **Login Security**.
2. Select the **RADIUS** tab, then fill in the fields for the primary server. A secondary server is optional.
3. Click **OK** or **Apply**.

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

**Set up the access control list**
Set up a list of IP addresses that can be allowed to access or blocked from accessing your ESM.
Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Login Security.
2. Click ACL Settings, then add IP addresses to the list.
3. Click OK to save the settings and close the Access Control List.

You can edit or remove IP addresses from the ACL list.

CAC settings
You can authenticate to the ESM by providing CAC credentials through the browser rather than by entering a user name and password.

CACs contain a client certificate that identifies the user, similar to the way a server certificate identifies a website. If you enable the CAC feature, we assume that you are familiar with CAC-based authentication. You know which browsers support this functionality and are familiar with the Electronic Data Interchange Personal Identifier (EDI-PI) associated with CACs.

Certificates are occasionally revoked. Certificate revocation lists (CRL) provide a way that systems can be made aware of these revocations. You can manually upload a .zip file containing CRL files.

ActivClient is the only supported CAC middleware on Windows. To use CAC authentication on the ESM from Windows using Internet Explorer, ActivClient must be installed on the client computer. Once ActivClient is installed, it is used to manage CAC credentials instead of the native Smart Card manager in Windows. The ActivClient software is most likely already installed if the client accesses other CAC-enabled websites. Instructions on setting up ActivClient and where to go to download the software can be obtained at http://militarycac.com/activclient.htm or from your organization's intranet.

When relying on CAC validation for application authenticity, the security of the system is dependent on the security of the Certificate Authority (CA). If the CA is compromised, CAC-enabled logins are also compromised.

Configure CAC login
To set up CAC login, you must enable the CAC login feature, upload the chain of CA root certificates, and enable a CAC user by setting the user name to the card holder's 10-digit EDI-PI. Once this is done, card holders can access the ESM in a CAC-enabled browser without being prompted for a user name or password.

ESM supports the Gemalto card reader. Please call McAfee Support If you need assistance with your card reader.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, click Login Security, then select the CAC tab.
2. Enter the information and make the selections requested, then click OK.
3. Enable each CAC user.
   a. On System Properties, click Users and Groups, then enter the system password.
   b. In the Users table, highlight the name of the user, then click Edit.
c  Replace the name in the **Username** field with the 10-digit EDI-PI.

d  (Optional) Enter the user's name in the **User Alias** field, then click **OK**.

**Configure Active Directory authentication settings**

You can configure the ESM to authenticate users to an Active Directory. When it is enabled, all users, except the system administrator, authenticate with the Active Directory. If authentication is disabled, users who are set up for Active Directory authentication can't access the system.

**Before you begin**

- Set up an Active Directory that can be accessed from the ESM.
- Create a group (see *Set up user groups*) with the same name as the Active Directory group that has access to the ESM. For example, if you name the group "McAfee Users," you must go to **System Properties | Users and Groups** and add a group named "McAfee Users."

**Task**

For option definitions, click **?** in the interface.

1  On the system navigation tree, select **System Properties**, then click **Login Security**.

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

3  Click **Add**, then add the information requested to set up the connection.

4  Click **OK** on the **Active Directory Connection** page.

**Set up user credentials for McAfee ePO**

You can limit access to a McAfee ePO device by setting up user credentials.

**Before you begin**

The McAfee ePO device must not be set up to require global user authentication (see *Set up global user authentication*).

**Task**

For option definitions, click **?** in the interface.

1  On the system navigation bar of the ESM console, click **options**, then select **ePO Credentials**.

2  Click the device, then click **Edit**.

3  Type the user name and password, test the connection, then click **OK**.

To access this device, users need the user name and password you added.

**Disable or re-enable a user**

If a user exceeds the allowed failed login attempts within the timeframe set in **Login Security**, use this feature to re-enable the account. You might also use this feature if you need to block user access temporarily or permanently without deleting the user from the system.
Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties | Users and Groups**.
2. In the **Users** table, highlight the user name, then click **Edit**.
3. Select or deselect **Disable account**, then click **OK**.

The icon next to the user name on **Users and Groups** reflects the status of the account.

Authenticate users to an LDAP server
You can configure the ESM to authenticate users to an LDAP server.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Login Security**.
2. Click the **LDAP** tab.
3. Fill in the fields, then click **Apply** or **OK**.

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

Set up user groups
Groups consist of users who inherit the settings of the group. When a group is added, devices, policies, and privileges must be assigned.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Users and Groups | Add**.
2. Fill in the information requested on each tab, then click **OK**.

The group is added to the **Groups** table on the **Users and Groups** page.

Add a group with limited access
To restrict specific users' access to features on the ESM, create a group that includes those users. This option limits their access to alarms, case management, ELM, reports, watchlists, asset management, policy editor, zones, system properties, filters, and the actions toolbar (see *Working with users and groups*). All other features are disabled.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, then click the **Properties** icon.
2. Click **Users and Groups**, then type the system password.
3 Do one of the following:
   • If the group is already set up, select it on the Group table, then click Edit.
   • If you are adding a group, click Add next to the Groups table, fill in the name and description, then select users.

4 Click Privileges, then select Limit access of this group.
   Most privileges are disabled.

5 From the remaining list of privileges, select the privileges that you want this group to have.

6 Click each tab and define the rest of the settings for the group.

---

**Backing up and restoring system settings**

Save current system configuration settings automatically or manually so they can be restored in case of system failure or data loss. You can also set up and save current settings to a redundant ESM.

A standard backup saves all configuration settings, including those for policy, as well as SSH, Network, and SNMP files. When you add a new ESM device, Backup & Restore is enabled to backup every 7 days. You can back up events, flows, and logs received by the system. The first backup of event, flow, or log data saves only data from the start of the current day. Subsequent backups save data starting at the time of the last backup.

> If you back up events, flows, or logs to the ESM, the disk space on the ESM is reduced. We recommend that you periodically download or delete backup files from the local ESM.

To restore the system, you can select one or more backup files on the ESM, a local computer, or a remote location to revert all of your settings and data to a previous state. When you perform this function, all changes made to the settings after the backup was created are lost. For example, if you are performing a daily backup and want to restore the data from the last three days, select the last three backup files. The events, flows, and logs from the three backup files are added to the events, flows, and logs that are currently on the ESM. All settings are then overwritten with the settings contained in the most recent backup.

**Back up ESM settings and system data**

There are multiple ways to back up the data on the ESM. When you add a new ESM, Backup & Restore is enabled to backup every seven days. You can disable it or make changes to the default settings.

**Task**

For option definitions, click ? in the interface.

1 On the system navigation tree, select System Properties, then click System Information | Backup & Restore.

2 Define the settings for any of these items:
   • Automatic backup
   • Manual backup
   • Redundant ESM
   • Restore the system to a previous backup

3 Click OK to close the Backup & Restore page.
See also

Restore ESM settings on page 179
Work with backup files on ESM on page 179

**Restore ESM settings**

In the case of system failure or data loss, you can restore your system to a previous state by selecting a backup file.

**Task**

If the database contains the maximum allowed records and the records being restored are outside of the range of current data on the ESM, the records are not restored. To save and access data outside of that range, you must have inactive partition archiving set up (see Set up data retention limits).

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click System Information | Backup & Restore | Restore Backup.
2. Select the type of restore you need to perform.
3. Select the file you want to restore or enter the information for the remote location, then click OK.

Restoring a backup can take a long time, based on the size of the restore file. The ESM is offline until the full restore is completed. During this time, the system tries to reconnect every 5 minutes. When the process is completed, the Login page appears.

See also

Set up data retention limits on page 170

**Restore backed up configuration files**

You can restore SSH, Network, SNMP and other configuration files that were backed up on the ESM for each device.

**Before you begin**

Back up configuration files on the ESM (see Back up ESM settings and system data).

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, click the device, then click the Properties icon.
2. Click the Configuration option for the device, click Restore Config, then click Yes on the confirmation page.

**Work with backup files on ESM**

The backup files that were saved to the ESM can be downloaded, deleted, or viewed. You can also upload files to add them to the list of backup files.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click File Maintenance.
2. In the Select Type drop-down list, select Backup Files.
3. Select the action you want to perform.
4. Click OK.

**See also**
*Back up ESM settings and system data on page 178*

**Manage file maintenance**
The ESM stores backup, software update, alarm log, and report log files. You can download, upload, and remove files from each of these lists.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click File Maintenance.
2. In the Select File Type field, select Backup Files, Software Update Files, Alarm Log Files, or Report Files.
3. Select the files, then click one of the options.
4. Click Apply or OK.

**See also**
*Back up ESM settings and system data on page 178*

**Redundant ESM**
The redundant ESM feature allows you to save current ESM settings to redundant ESM that can be converted to the primary ESM in case of system failure or data loss. This feature is only available to users with system administrator privileges.

Once you set up a redundant ESM, the configuration and policy data from the primary ESM is automatically synced every five minutes with the redundant ESM. To set up a redundant ESM you must define the settings for the redundant device, which receives the settings and data from the primary device, and define the settings for the primary device, which sends the backup settings and data to the redundant device. The redundant ESM must be configured before the primary ESM can connect to it.

> The ESM redundancy feature is not available on an ESMREC combo device.

**Set up redundant ESM**
To save your system settings on a redundant ESM, you must set up each ESM so they communicate with each other.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click System Information | Backup & Restore | Redundancy.
2. In the ESM Type field, ensure that Primary is selected.
3. Enter the information for the primary ESM, then select or add the redundant ESMs.
   
   You can add a maximum of five redundant ESMs.
4. Select the **Redundant** radio button, then type the IP address for the primary ESM and select the SSH port.
5. Click OK.
   
   You are warned that a service restart is required which causes all users to lose their connection to the ESM.
6. Click Yes to continue with the sync.

**Replace a redundant ESM**

If a redundant ESM quits working, you can replace it with a new one.

**Before you begin**

Add the new redundant ESM to the system.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, and make sure that System Information is selected.
2. Click Backup & Restore | Redundancy, then select Primary and type the new redundant IP address in the Redundant ESM IP Address field.
3. Select Redundant and make sure that the primary ESM IP address is correct.
4. Select Primary, then click Connect to verify that the two devices are communicating.
5. Select Sync Entire ESM, then click OK.

**Managing the ESM**

You can perform several operations to manage the software, logs, certificate, feature files, and communication keys for the ESM.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>Manage Logs</td>
<td>Configure the types of events that are logged on the event log.</td>
</tr>
<tr>
<td></td>
<td>ESM Hierarchy</td>
<td>Configure data options when working with hierarchical ESM devices.</td>
</tr>
<tr>
<td></td>
<td>Obfuscation</td>
<td>Define global settings to mask selected data on any alert record that is sent out in event forwarding or sent to a parent ESM.</td>
</tr>
<tr>
<td>Tab</td>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logging</td>
<td></td>
<td>Send internal events to the ELM for storage. This data can be used for auditing.</td>
</tr>
<tr>
<td>System Locale</td>
<td></td>
<td>Select the system language to use for logging events such as health monitor and device log.</td>
</tr>
<tr>
<td>Name Map</td>
<td></td>
<td>Deselect the ports and protocols to have them display raw numbers instead of names. For example, if you deselect Source Port or Destination port, http:80 displays as 80. If you select Protocols, raw number 17 displays as udp.</td>
</tr>
<tr>
<td>Key Management</td>
<td>Certificate</td>
<td>Install a new Secure Socket Layer (SSL) certificate.</td>
</tr>
<tr>
<td>Regenerate SSH</td>
<td></td>
<td>Regenerate the private or public SSH key pair to communicate with all devices.</td>
</tr>
<tr>
<td>Export All Keys</td>
<td></td>
<td>Export the communication keys for all devices on the system, instead of exporting them one at a time.</td>
</tr>
<tr>
<td>Restore All Keys</td>
<td></td>
<td>Restore the communication keys for all or selected devices, which were exported using the Export All Keys function.</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Update ESM</td>
<td>Update ESM software from the McAfee rules and updates server or a McAfee security engineer.</td>
</tr>
<tr>
<td>ESM Data</td>
<td></td>
<td>Download a .tgz file that contains information regarding the status of the ESM. This status can assist McAfee Support troubleshoot and resolve issues.</td>
</tr>
<tr>
<td>Task manager</td>
<td></td>
<td>View the queries running on the ESM and stop them, if needed.</td>
</tr>
<tr>
<td>Shutdown</td>
<td></td>
<td>Shut down the ESM. You are warned that this action causes all users to lose communication with the ESM.</td>
</tr>
<tr>
<td>Reboot</td>
<td></td>
<td>Stop and restart the ESM. You are warned that this action causes all users to lose communication with the ESM.</td>
</tr>
<tr>
<td>Terminal</td>
<td></td>
<td><strong>This feature is for advanced users only.</strong> Enter Linux commands on the ESM. The terminal is only a partial batch mode emulator and not all commands are available. • The terminal doesn't keep a present working directory. • You can't use cd to go to another directory. • Full path names must be used. • The &gt; or &gt;&gt; operators do not work; all results are returned to the screen.</td>
</tr>
<tr>
<td>Get Features</td>
<td></td>
<td>If you have purchased additional features, enable them on your ESM by downloading an encrypted file that contains information about features that your ESM supports.</td>
</tr>
<tr>
<td>Set Features</td>
<td></td>
<td>Install the file you downloaded with Get features.</td>
</tr>
</tbody>
</table>
### Tab | Option | Definition
--- | --- | ---
**Connect** | **Give McAfee support access to your system when you call for support.**
 &nbsp; &nbsp; &nbsp; **This option is not FIPS-compliant and is not available when operating in FIPS mode.**
**View Statistics** | **Access the following information for any ESM device:**
 &nbsp; &nbsp; &nbsp; **• Memory and swap space utilization statistics.**
 &nbsp; &nbsp; &nbsp; **• CPU utilization.**
 &nbsp; &nbsp; &nbsp; **• System switching activity.**
 &nbsp; &nbsp; &nbsp; **• Input/output and transfer rate statistics.**
 &nbsp; &nbsp; &nbsp; **• Queue length and load averages.**

---

### See also
- *Access a remote device* on page 187
- *Regenerate SSH key* on page 185
- *Manage recipients* on page 154
- *Types of events* on page 183
- *Manage logs* on page 183
- *Install a new certificate* on page 162
- *Set up ESM logging* on page 184
- *Mask IP addresses* on page 184
- *Export and restore communication keys* on page 185
- *Available Linux commands* on page 187
- *Use Linux commands* on page 187

### Manage logs
There are several types of events that are generated on the ESM. You can select the ones you want saved in the event log.

#### Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **ESM Management**.
2. Click **Manage logs**, then select the event types you want to log.
3. Click **OK**.

#### Types of events
These are the event log types generated on the ESM.

| Event type | Events logged |
--- | --- |
**Authentication** | Login, logout, and user account changes.  
 &nbsp; &nbsp; &nbsp; **To be in compliance with FIPS regulations, Authentication Mode is always set to None.**
**Backup** | Database backup process.  
**Blacklist** | Blacklist entries sent to the device.  
**Device** | Any device changes or communications such as getting events, flows, and logs.  
**Event Forwarding** | Event forwarding changes or errors.  

<table>
<thead>
<tr>
<th>Event type</th>
<th>Events logged</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Monitor</td>
<td>Device status events.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Notification changes or errors.</td>
</tr>
<tr>
<td>Policy</td>
<td>Policy management and applying policies.</td>
</tr>
<tr>
<td>Rule Server</td>
<td>Download and validation of rules downloaded from the rule server.</td>
</tr>
<tr>
<td>System</td>
<td>System setting changes and table rollover logging.</td>
</tr>
<tr>
<td>Views</td>
<td>Changes to views and queries.</td>
</tr>
</tbody>
</table>

**Mask IP addresses**

You can select to mask specific data on event records sent out in event forwarding or to a parent ESM.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click ESM Management | ESM Hierarchy.
2. Select Obfuscate for the ESMs that you want to mask data on.
   
   The Obfuscation Fields Selection page opens.
3. Select the fields that you want to mask.
4. Click OK.

Once this is set up, if a parent ESM requests a packet from a child ESM, the data you selected is masked.

**Set up ESM logging**

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

**Before you begin**

Add an ELM device to your system.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click ESM Management.
2. On the Configuration tab, click Logging.
3. Make the requested selections, then click OK.

**Change language for event logs**

When you logged on to ESM for the first time, you selected the language to be used for event logs such as the health monitor log and device log. You can change this language setting.
Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select System Properties | ESM Management.
2 Click System Locale, select a language from the drop-down list, then click OK.

Export and restore communication keys
Export the communication keys for all devices on the system to a single file. Once you export the communication keys, you can restore them when needed.

- On the system navigation tree, select System Properties | ESM Management, then click the Key Management tab.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export all communication keys</td>
<td>1 Click Export All Keys.</td>
</tr>
<tr>
<td></td>
<td>2 Set the password for the keys file, then click OK.</td>
</tr>
<tr>
<td></td>
<td>3 Select the location to save the file, then click Save.</td>
</tr>
<tr>
<td>Restore all communication keys</td>
<td>1 Click Restore All Keys.</td>
</tr>
<tr>
<td></td>
<td>2 Locate the file you set up when you exported the keys, then click Open.</td>
</tr>
<tr>
<td></td>
<td>3 Click Upload, then enter the password you set.</td>
</tr>
<tr>
<td></td>
<td>4 Select the devices you need to restore, then click OK.</td>
</tr>
</tbody>
</table>

Regenerate SSH key
Regenerate the private or public SSH key pair to communicate with all devices.

Task
For option definitions, click ? in the interface.

1 On the system navigation tree, select System Properties, then click ESM Management.
2 On the Key Management tab, click Regenerate SSH.
   You are warned that the new key replaces the old key.
3 Click Yes.

When the key is regenerated, it replaces the old key pair on all the devices managed by the ESM.

Queries task manager
If you have administrator or master user rights, you can access the Task Manager, which displays the list of queries running on the ESM. From here, you can close specific queries if they affect system performance. Long running queries have a higher likelihood of affecting performance.

The intent of this feature is to troubleshoot ESM runtime issues, not to close queries. Use this feature with assistance from McAfee support.

Characteristics of the task manager include:
• You can close report, view, watchlist, execute and export, alarm, and external API queries on the system. You cannot close system queries.

• When you click a query, the details are displayed in the **Query Details** area.

• By default, the list refreshes automatically every five seconds. If you select a query and the list auto-refreshes, it remains selected and the details are updated. If the query is complete, it no longer appears on the list.

• If you do not want the list to auto-refresh, deselect **Auto refresh list**.

• To view system tasks, which are tasks that haven't been identified yet, deselect **Hide system tasks**.

• The columns on the table can be sorted.

• You can select and copy the data in the **Query Details** area.

• If a query can be closed, it has a delete icon \( \times \) in the last column. When you click it, a dialog box requests confirmation.

**Manage queries running on ESM**

The **Task Manager** displays a list of the queries that are running on the ESM. You can view their status and delete any that affect system performance.

**Task**

For option definitions, click \( ? \) in the interface.

1. On the system navigation tree, select the system, then click the **Properties** icon \( \text{ inflammable } \).

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

3. Review and take action on the list of running queries.

**Update primary or redundant ESM**

If you are updating a primary or redundant ESM, you must follow specific steps to avoid losing the event, flow, and log data.

**Task**

For option definitions, click \( ? \) in the interface.

1. Disable the collection of alerts, flows, and logs.
   a. On the system navigation tree, select **System Information**, then click **Events, Flows, & Logs**.
   b. Deselect **Auto check every**.

2. Update the primary ESM.

3. Update the redundant ESM. This takes additional time if there are redundancy files to process.

4. Enable the collection of alerts, flows, and logs by selecting **Auto check every** once again.

   If the update fails, see **Update to version 9.3**.
**Access a remote device**

If a device is set up at a remote location, use the Terminal option to run Linux commands to see the device. This feature is for advanced users and must be used under the direction of McAfee Support personnel for emergency situations.

This option is not FIPS-compliant and is disabled in FIPS mode.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click ESM Management.
2. On the Maintenance tab, click Terminal.
3. Enter the system password, then click OK.
4. Enter Linux commands as needed and export to save the contents to a file.

The export doesn't include results that were cleared from the Terminal page during the current terminal session.

5. Click Close.

**See also**

Available Linux commands on page 187

**Use Linux commands**

You can use the Terminal option to enter Linux commands on the ESM. This feature is for advanced users. Use it only under the direction of McAfee support for an emergency.

This option is not FIPS-compliant and is disabled in FIPS mode.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click ESM Management.
2. On the Maintenance tab, click Terminal, type the system password, then click OK.
3. Type Linux commands (see Available Linux commands).
4. Click Clear to delete the contents of the page, if needed.
5. (Optional) Click Export to save the contents to a file.

The export doesn't include results that were cleared from the terminal page during the current terminal session.

**Available Linux commands**

These are the commands available on the Terminal page.

**Terminal page commands**

- getstatsdata
- ps
- echo
- date
These are the available commands that are modified before execution.

<table>
<thead>
<tr>
<th>This command...</th>
<th>Changed to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>II</td>
<td>ll--classify</td>
</tr>
<tr>
<td>ping</td>
<td>ping -c 1</td>
</tr>
<tr>
<td>ls</td>
<td>ls--classify</td>
</tr>
<tr>
<td>top</td>
<td>top -b -n 1</td>
</tr>
<tr>
<td>ping6</td>
<td>ping6 -c 1</td>
</tr>
</tbody>
</table>

For information about the getstatsdata command, see *Gather statistical data for troubleshooting* in Appendix D. For information about all other commands, see [http://www.linuxmanpages.com](http://www.linuxmanpages.com).

### Using a global blacklist

A blacklist is a way to block traffic as it flows through a Nitro IPS or virtual device before it is analyzed by the deep packet inspection engine.

You can use the Nitro IPS Blacklist option to set up a blacklist for individual Nitro IPS devices on the ESM. With Global Blacklist, you can set up a blacklist that applies to all Nitro IPS devices managed by the ESM. This feature only allows permanent blacklist entries. To set up temporary entries, you must use the Nitro IPS Blacklist option.

Each Nitro IPS and virtual device can use the global blacklist. The feature is disabled on all devices until you enable it.
The **Global Blacklist Editor** page includes three tabs:

- **Blocked Sources** — Matches against the source IP address of traffic passing through the device.
- **Blocked Destinations** — Matches against the destination IP address of traffic passing through the device.
- **Exclusions** — Provides immunity from being automatically added to either of the blacklists. Critical IP addresses (for example, DNS and other servers or system administrators' workstations) can be added to the exclusions to ensure that they are never automatically blacklisted regardless of the events they might generate.

Entries in both **Blocked Sources** and **Blocked Destinations** can be configured to narrow the effect of the blacklist to a specific destination port.

When adding entries:

- **Add** is enabled when you change the IP address or the port.
- Entries in the **Blocked Sources** and **Blocked Destinations** lists can be configured to blacklist on all ports, or a specific port.
- Entries that use a masked range of IP addresses must be configured with the port set to any (0) and the duration must be permanent.
- While these lists require IP address format, there are a few tools included to help add meaning to these addresses. After typing an IP address or host name in the **IP Address** field, the button next to that control says either **Resolve** or **Lookup** based on the value entered. If it says **Resolve**, clicking on it resolves the entered host name, populates the **IP Address** field with that information, and moves the host name to the **Description** field. Otherwise, clicking **Lookup** performs a lookup on the IP address and populates the **Description** field with the results of that lookup.

Some websites have more than one IP address, or have IP addresses that are not always the same. Don't rely on this tool to ensure blocking of some websites.

### Set up a global blacklist

Set up a global blacklist that is common to all the devices you select so you don't have to enter the same information on multiple devices.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Global Blacklist**.
2. Select the **Blocked Sources**, **Blocked Destinations**, or **Exclusions** tab, then manage blacklist entries.
3. Select the devices that must use the global blacklist.
4. Click **Apply** or **OK**.

### What is data enrichment

You can enrich events sent by the upstream data source with context not in the original event (such as an email address, phone number, or host location information). This enriched data becomes part of the parsed event and is stored with the event just like the original fields.

Set up data enrichment sources by defining how to connect to the database and access one or two table columns within that database. Then define which devices receive the data and how to enrich that data, both events and flows.
You can also edit or remove data enrichment sources, as well as run a query on the Data Enrichment page. To do so, select the source and click Edit, Remove, or Run Now.

Events that trigger on the ESM are not enriched. Data acquisition takes place on the ESM, not on the devices.

There is a connector to the relational data source in Hadoop HBase, using 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**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Data Enrichment | Add.
   
   Tabs and fields on the Data Enrichment Wizard vary based on the enrichment type you select.

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

3. Click Finish, then click Write.

4. Select the devices you want to write the data enrichment rules to, then click OK.

**Set up McAfee Real Time for McAfee ePO™ data enrichment**
When you select the McAfee Real Time for McAfee ePO source on the Data Enrichment Wizard, you can test your query and choose the columns for Lookup and Enrichment.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click the Properties icon.

2. Click Data Enrichment, then click Add and complete the information on the Main tab.

3. On the Source tab, select Real Time for ePO in the Type field, select the device, then click the Query tab.

4. Add the information requested, then click Test.

If the query doesn't generate the information you need, make adjustments to the settings.

**Add Hadoop HBase data enrichment source**
Pull HBase identity mapping through a Receiver to enrich events by adding Hadoop HBase as a data enrichment source.

**Task**
For option definitions, click ? in the interface.

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:

   ```xml
   <Scanner batch="1024">
   <filter>
   { "type": "SingleColumnValueFilter", "op": "EQUAL", "family": "ZW1wbG95ZWVJbmZv", "qualifier": "dXNlcm5hbWU=", "latestVersion": true, "comparator": { "type": "BinaryComparator", "value": "c2NhcGVnb2F0" } }
   </filter>
   </Scanner>
   ```

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

**Add Hadoop Pig data enrichment source**

You can leverage Apache Pig query results to enrich Hadoop Pig events.

**Task**

For option definitions, click ? in the interface.

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.
On the Scoring tab, set the score for each value returned from the single column query.

On the Destination tab, select the devices to which you want to apply enrichment.

Add Active Directory data enrichment for user names
You can leverage Microsoft Active Directory to populate Windows events with the full user display names.

**Before you begin**
Verify that you have the System Management privilege.

For option definitions, click ? in the interface.

**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_Nichname 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.
Managing cyber threats

McAfee ESM allows you to retrieve indicators of compromise (IOC) from remote sources and quickly access related IOC activity in your environment.

Cyber threat management enables you to set up automatic feeds that generate watchlists, alarms, and reports, giving you visibility to actionable data. For example, you can set up a feed that automatically adds suspicious IP addresses to watchlists to monitor future traffic. That feed can generate and send reports indicating past activity. Use Event Workflow views > Cyber Threat Indicators views to drill down quickly to specific events and activity in your environment.

Contents

- Set up cyber threat management
- View cyber threat feed results

Set up cyber threat management

Set up feeds to retrieve indicators of compromise (IOC) from remote sources. You can then use these feeds to generate watchlists, alarms, and reports that allow users to access related IOC activity in your environment.

Before you begin

Verify that you have the following permissions:

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

Task

For option definitions, click ? in the interface.

1 On the system navigation tree, click System Properties.

2 Click Cyber Threat Feeds, then click Add.

3 On the Main tab, enter the feed name.
4 On the **Source** tab, select the source data type and its connection credentials. Click **Connect** to test the connection.

Supported sources include McAfee Advanced Threat Defense and MITRE Threat Information Exchange (TAXII).

5 On the **Frequency** tab, identify how often the feed pulls the IOC files (pull frequency). Available pull frequencies include: every x minutes, daily, hourly, weekly, or monthly. Specify the daily trigger time.

6 On the **Watchlist** tab, select which property or field in an IOC file to append to an existing watchlist. You can add watchlists for any supported property or field.

If the watchlist you need does not yet exist, click **Create New Watchlist**.

7 On the **Backtrace** tab, identify which events (default) and flows to analyze, matching data to analyze, and how far back to analyze data against this feed.

   a. Choose to analyze events, flows, or both.

   b. Indicate how far back (in days) to analyze the events and flows.

   c. Specify what action you want ESM to take if the backtrace finds a data match.

   d. For alarms, select an assignee and severity.

8 Return to the **Main** tab, then select **Enabled** to activate this feed.

9 Click **Finish**.

**See also**

*View cyber threat feed results on page 194*

---

### View cyber threat feed results

View indicators of compromise (IOC) from external data sources, identified by your organization’s cyber threat feeds. Quickly drill down to the threat details, file descriptions, and corresponding events for each indicator source.

**Before you begin**

Verify that you have the Cyber Threat User permission, which allows you to view the results of your organization's cyber threat feeds.

**Task**

For option definitions, click ? in the interface.

1. On the ESMconsole, **Default Summary**, select Event Workflow Views | Cyber Threat Indicators.

2. Choose the time period for the view.

3. Filter by feed name or supported IOC data types.

4. 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.

Drill down to threat details using the Description, Details, Source Events, and Source Flows tabs

See also

Set up cyber threat management on page 193
Managing cyber threats
View cyber threat feed results
Working with content packs

When a specific threat situation occurs, respond immediately by importing and installing the relevant content pack from the rules server. Content packs contain use-case driven correlation rules, alarms, views, reports, variables, and watchlists to address specific malware or threat activity. Content packs enable you to respond to threats without wasting time creating tools from scratch.

**Import content packs**

McAfee creates use-case driven content packs, complete with correlation rules, alarms, views, reports, variables, or watchlists to address specific malware activity.

**Before you begin**

Verify that you have the following permissions:

- System Management
- User Administration

**Task**

For option definitions, click ? in the interface.

1. Check for rule updates on page 22

   - Online users receive available content packs automatically as part of rules updates. Offline users must download and import individual content packs manually from the rules hosting site.

2. On the system navigation tree, click **System Properties**.

3. Click **Content Packs**.
4 To import and install a new content pack, click **Browse**.

   - **i** Checking for rules updates automatically downloads any new or updated content packs.

   a Click **Import** and browse to the content pack file you want to import.

   b Click **Upload**.

   A message indicates the status of the import.

   c Click the content pack to review the details of what is included in that pack.

   d Select the wanted pack, then select to install that content pack.

5 To update or uninstall an existing content pack, check the wanted pack and click **Update** or **Uninstall**.

   - **i** Use caution when updating existing content packs. If you previously customized any content pack elements, the update might overwrite those customized elements.

6 To uninstall an existing content pack, check the wanted pack and click **Uninstall**.
6

Working with alarms

Contents

- How ESM alarms work
- Create an alarm
- Enable or disable alarm monitoring
- Customize summary for triggered alarms and cases
- Manage alarm message templates
- Manage alarm audio files
- Manage alarm recipients
- Manage alarms

How ESM alarms work

You can configure the system to provide real-time alarms.

When an alarm is triggered, it is automatically added to the Alarms log, located under the system navigation tree, as well as to the Triggered Alarms View. You can also configure an alarm action to:

- Log an event to the ESM
- Provide a visual and auditory alert.
- Create a case for a specific person or group.
- Update a watchlist.
- Send an event to remedy.
- Send a text or email.
- Execute a script.

The Alarms log pane shows the total number of alarms currently listed, by severity:

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Severity</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>high</td>
<td>66–100</td>
</tr>
<tr>
<td></td>
<td>medium</td>
<td>33–65</td>
</tr>
<tr>
<td></td>
<td>low</td>
<td>1–32</td>
</tr>
</tbody>
</table>
Once an alarm is added, it begins to trigger when the conditions are met. If you set the **Maximum Condition Trigger Frequency** to 15 minutes, the first alarm triggers when the number of events specified in **Event Count** occur within a 15-minute period. Events that come in during the first 15 minutes don’t trigger the alarm.

You can acknowledge, delete, and view details of any of the triggered alarms. When you acknowledge a triggered alarm, it no longer appears on the **Alarms** log, but is still listed on the **Triggered Alarms** view. When you delete an alarm, it is removed from the **Alarms** log as well as from the **Triggered Alarms** view.

If you select the **Visual Alert** action on the **Alarm Settings** page, the visual alert closes after 30 seconds if it hasn’t been closed, acknowledged, or deleted. The audio alert you select plays until you close, acknowledge, or delete the visual alert or click the audio icon to stop the audio alert.

![Information](image)

You can select whether to show the **Alarms** log pane on the **Options** page (see **Select user settings**).

See also

**Select user settings** on page 27

---

**Create an alarm**

Add an alarm so it triggers when the conditions you define are met.

### Before you begin

You must have administrator rights or belong to an access group with the **Alarm Management** privilege.

### Task

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Alarms | Add**.

2. Complete the information on the **Summary**, **Condition**, **Actions**, and **Escalation** tabs.

   ![Information](image)

   See **UCAPL alarms** for a list and description of alarms to help you meet Unified Capabilities Approved Products List (UCAPL) requirements.

3. Click **Finish**.

   The alarm is added to the list on the **Alarms** page and is triggered when its conditions are met.
Tasks

- **Set up correlation alarm to include source events on page 203**
  If you add tags to an Internal Event Match alarm that uses a correlation event as the match, the source events information is included in the results.

- **Add a Field Match alarm on page 203**
  A Field Match alarm matches on multiple fields of an event, and triggers as soon as the device receives and parses the event.

- **Add an alarm to rules on page 204**
  To be notified when events are generated by specific rules, you can add an alarm to those rules.

- **Create an SNMP trap as an action in an alarm on page 163**
  You can send SNMP traps as an action within an alarm.

- **Add a power failure notification alarm on page 164**
  Add an alarm to notify you when either of the ESM power supplies fail.

- **Add a health monitor event alarm on page 206**
  Health monitor rules generate events that appear under a base device in the system navigation tree.

- **Copy an alarm on page 213**
  You can use an existing alarm as a template for a new alarm by copying and saving it with a different name.

UCAPL alarms

You can add several alarm types to meet UCAPL requirements.

See *Create an alarm* to set up the general alarm settings then follow the steps in this table.

<table>
<thead>
<tr>
<th>Alarm type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjustable threshold for failed logins reached</td>
<td>To trigger an alarm when an adjustable threshold is reached for a number of failed logins for the same user, create an Internal Event Match alarm matching on Signature ID, then enter a value of 306-36.</td>
</tr>
<tr>
<td>Threshold for no activity reached</td>
<td>To trigger an alarm when a user account is locked because the no-activity threshold is reached, create an Internal Event Match alarm matching on Signature ID, then enter a value of 306-35.</td>
</tr>
<tr>
<td>Allowed concurrent sessions reached</td>
<td>To trigger an alarm if a user attempts to log on to the system after the number of allowed concurrent sessions has been reached, create an Internal Event Match alarm matching on Signature ID, then enter a value of 306-37.</td>
</tr>
<tr>
<td>Failed system file integrity check</td>
<td>To trigger an alarm in the event of a failed system file integrity check, create an Internal Event Match alarm matching on Signature ID, then enter a value of 306-50085.</td>
</tr>
<tr>
<td>Certificates are about to expire</td>
<td>To trigger an alarm when common access card (CAC) or web server certificates are about to expire, create an Internal Event Match alarm matching on Signature ID, then enter a value of 306-50081, 306-50082, 306-50083, 306-50084.</td>
</tr>
</tbody>
</table>

The alarm triggers 60 days prior to expiration and then on a weekly basis thereafter. The number of days is not configurable at this time.
<table>
<thead>
<tr>
<th>Alarm type</th>
<th>Description</th>
</tr>
</thead>
</table>
| SNMP trap sent when system state not approved | To configure an SNMP trap as an alarm action so that a trap is sent to the NMS when it detects that the system is no longer operating in an approved or secure state, do this:  
1. Create an alarm matching on any condition, then go to the Actions tab and select Send Message.  
2. Click Add Recipients | SNMP, select the recipient, then click OK.  
3. In the Send Message field, click Configure, click Templates, then click Add.  
4. Select SNMP Template in the Type field, enter the text for the message, then click OK.  
5. On the Template Management page, select the new template, then click OK.  
6. Complete the remaining alarm settings. |
| Syslog message sent when system state not approved | To configure a syslog message as an alarm action so that a syslog message is sent to the NMS when it detects that the system is no longer operating in an approved or secure state, do this:  
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 | To configure an SNMP trap to be sent to notify an appropriate Network Operations Center (NOC) within 30 seconds if a security log fails to record required events, do the following:  
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.  
SNMP traps are sent to the SNMP profile recipient with the message "Failed to write to the security log." |
| Audit functions start up or shut down | To configure an SNMP trap to be sent when the audit functions (such as the database, cpservice, IPSDBServer) start up or shut down, access SNMP traps or SNMP Settings (see previous item), 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 | To trigger an alarm when an administrative session exists for each of the defined administrative roles, create an Internal Event Match alarm matching on Signature ID, then 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. |

See also

Create an alarm on page 200
Set up correlation alarm to include source events

If you add tags to an Internal Event Match alarm that uses a correlation event as the match, the source events information is included in the results.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, then click the Properties icon.
2. Click Alarms, click the Settings tab, then click Templates.
3. On the Template Management page, click Add, then complete the information requested.
4. 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.
5. 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 message body field looks like the following example if you include the source IP, destination IP, and severity of the event in the message:

Alarm: [$Alarm Name]
Assignee: [$Alarm Assignee]
Trigger Date: [$Trigger Date]

Summary: [$Alarm Summary]
[source_events_start]
Source IP: [$Source IP]
Dest IP: [$Destination IP]
Severity: [$Average Severity]
[source_events_end]

If the alarm is not triggered by a correlated event, the message does not include the data.

Add a Field Match alarm

A Field Match alarm matches on multiple fields of an event, and triggers as soon as the device receives and parses the event.

The alarm condition that was previously called Field Match is now called Internal Event Match.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, click the Properties icon, then click Alarms.
2. Click Add, type the alarm name and select the assignee, then click the Condition tab.
3. In the **Type** field, select **Field Match**, then set up the conditions for the alarm.
   a. Drag-and-drop the **AND** or **OR** icon (see **Logic Elements** in the Product Guide) to set up the logic for the alarm’s condition.
   b. Drag-and-drop the **Match Component** icon onto the logic element, then complete the **Add Filter Field** page.
   c. In the **Maximum Condition Trigger Frequency** field, select the amount of time to allow between each condition to prevent a flood of notifications. Each trigger only contains the first source event that matches the trigger condition, not the events that occurred within the trigger frequency period. New events that match the trigger condition do not cause the alarm to trigger again until after the maximum trigger frequency period.

   If you set it to zero, all events generate an alarm.

4. 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).

5. Click the **Actions** and **Escalation** tabs and define the settings, then 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**.

---

**Add an alarm to rules**

To be notified when events are generated by specific rules, you can add an alarm to those rules.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, click the **Policy Editor** icon on the actions toolbar.

2. Select the type of rule in the **Rule Types** pane.

3. Select one or more rules in the rules display area.

4. Click the **Alarms** icon.

5. Define the alarm’s settings.

**See also**

*Create an alarm on page 200*

---

**Create an SNMP trap as an action in an alarm**

You can send SNMP traps as an action within an alarm.

**Before you begin**

Prepare the SNMP trap Receiver (only required if you don’t have an SNMP trap Receiver).

For option definitions, click ? in the interface.
Task
1. Create an SNMP profile to tell the ESM where to send the SNMP traps.
   a. On the system navigation tree, select the system then click the Properties icon.
   b. Click Profile Management, then select SNMP Trap in the Profile Type field.
   c. Fill in the remaining fields, then click Apply.

2. Configure SNMP on the ESM.
   a. On System Properties, click SNMP Configuration, then click the SNMP Traps tab.
   b. Select the port, select the types of traps to send, then select the profile you added in Step 1.
   c. Click Apply.

3. Define an alarm with SNMP Trap as an action.
   a. On System Properties, click Alarms, then click Add.
   b. Fill in the information requested on the Summary, Condition, and Devices tabs, selecting Internal Event Match as the condition type, then click the Actions tab.
   c. Select Send Message, then click Configure to select or create a template for SNMP messages.
   d. Select Basic SNMPTrap in the SNMP field, or click Templates, then click Add.
   e. Select an existing template or click Add to define a new template.
   f. Return to the Alarm Settings page, then proceed with alarm setup.

Add a power failure notification alarm
Add an alarm to notify you when either of the ESM power supplies fail.

Before you begin
Set up a General Hardware Failure SNMP trap (see Set up SNMP trap for power failure notification).

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, then click the Properties icon.

2. Click Alarms, click Add, add the requested data on the Summary tab, then click the Condition tab.

3. In the Type field, select Internal Event Match.

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

5. Fill in the remaining information on each tab as needed, then click Finish.

An alarm triggers when a power supply fails.
Add a health monitor event alarm

Health monitor rules generate events that appear under a base device in the system navigation tree. The signature IDs of the health monitor events can be used in the Values field of a Internal Event Match alarm to generate an alarm based on health monitor events. The Health Monitor Event Summary report is then generated as the alarm’s action.

For option definitions, click ? in the interface.

- There are a couple of ways to set up a health monitor event alarm.

<table>
<thead>
<tr>
<th>To set up an alarm...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before a health monitor event is generated</td>
<td>1 Follow the process to create an alarm (see Create an alarm).</td>
</tr>
<tr>
<td></td>
<td>2 On the system navigation tree, click Condition, then select the Internal Event Match type.</td>
</tr>
<tr>
<td></td>
<td>3 On the Field line, select Signature ID.</td>
</tr>
<tr>
<td></td>
<td>4 In the Values field, enter the signature ID for the health monitor rules (see Health monitor signature IDs).</td>
</tr>
<tr>
<td></td>
<td>5 Complete the remaining information as described in Create an alarm.</td>
</tr>
<tr>
<td>If a health monitor event already exists</td>
<td>1 On the system navigation tree, click the base device for the system event (Event Analysis or Default Summary).</td>
</tr>
<tr>
<td></td>
<td>2 Click the event, then click the Menu icon.</td>
</tr>
<tr>
<td></td>
<td>3 Select Actions</td>
</tr>
<tr>
<td></td>
<td>4 Fill out the remaining settings for the alarm.</td>
</tr>
</tbody>
</table>

See also
Create an alarm on page 200

Health monitor signature IDs

This list describes the health monitor rules and their signature IDs, type, device, and severity. Use these rules to create an alarm that notifies when a health monitor rule event is generated.

<table>
<thead>
<tr>
<th>Rule name</th>
<th>Signature ID</th>
<th>Description</th>
<th>Type</th>
<th>Device</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>A physical network interface connection has been made or removed</td>
<td>306-50080</td>
<td>Network interface settings modified, via an SSH session.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>A RAID error has occurred</td>
<td>306-50054</td>
<td>RAID errors encountered.</td>
<td>Hardware Monitor</td>
<td>All</td>
<td>High</td>
</tr>
<tr>
<td>Account disabled due to inactivity</td>
<td>306-35</td>
<td>User account disabled, due to inactivity.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>Account disabled due to max login failures</td>
<td>306-36</td>
<td>User account disabled, due to maximum logon failures.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>Add/Edit Remote Command</td>
<td>306-60</td>
<td>Alarm remote command added or deleted.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Rule name</td>
<td>Signature ID</td>
<td>Description</td>
<td>Type</td>
<td>Device</td>
<td>Severity</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>Advanced Syslog Parser collector state change alert</td>
<td>306-50029</td>
<td>ASP parser stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>APM distiller process</td>
<td>306-50066</td>
<td>ADM PDF/DOC text extraction engine stopped or started.</td>
<td>Software Monitor</td>
<td>APM</td>
<td>Medium</td>
</tr>
<tr>
<td>Approved configuration mismatch</td>
<td>146-7</td>
<td>Network discovery device change approved.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Archive configuration change</td>
<td>306-3</td>
<td>ESM archival settings changed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Archive process state change alert</td>
<td>306-50051</td>
<td>Receiver archiving process stopped or started.</td>
<td>Software Monitor</td>
<td>APM/REC/IPS/DBM</td>
<td>Medium</td>
</tr>
<tr>
<td>Asset vulnerable to event</td>
<td>146-10, 306-10</td>
<td>Vulnerability event created.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Audit administrator user login</td>
<td>306-38</td>
<td>UCAPL event, audit administrator logon.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Backup configuration change</td>
<td>306-1</td>
<td>ESM backup configuration settings modified.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Backup performed</td>
<td>306-2</td>
<td>Backup performed on the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Blue Martini parser alert</td>
<td>306-50071</td>
<td>Blue Martini parser stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Bypass NIC state alert</td>
<td>306-50001</td>
<td>NIC entered or exited bypass status.</td>
<td>Software Monitor</td>
<td>IPA/ADM/IPS</td>
<td>Medium</td>
</tr>
<tr>
<td>CAC cert has expired</td>
<td>306-50082</td>
<td>ESM CAC certificate expired.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>CAC cert will expire soon</td>
<td>306-50081</td>
<td>ESM CAC certificate expires soon.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>Case modified</td>
<td>306-70</td>
<td>Case modified.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Case status added/modified/deleted</td>
<td>306-73</td>
<td>Case status changed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Communication channel state change alert</td>
<td>306-50013</td>
<td>Control channel stopped or started.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>Configuration capture failed (device error)</td>
<td>146-4</td>
<td>Network discovery device error.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Configuration capture failed (device unreachable)</td>
<td>146-3</td>
<td>Network discovery device unreachable.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Configuration captured</td>
<td>146-5</td>
<td>Network discovery configuration checked successfully.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Configuration policy failure</td>
<td>146-8</td>
<td>Not used in system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Configuration policy pass</td>
<td>146-9</td>
<td>Not used in system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Rule name</td>
<td>Signature ID</td>
<td>Description</td>
<td>Type</td>
<td>Device</td>
<td>Severity</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Data allocation configuration change</td>
<td>306-7</td>
<td>ESM data allocation settings changed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>Data partitions free disk space alert</td>
<td>306-50005</td>
<td>Free space on each partition is low (for example, hada_hd has 10% free space).</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>Data retention configuration change</td>
<td>306-6</td>
<td>ESM data retention configuration changed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>Database detection services state alert</td>
<td>306-50036</td>
<td>DBM auto detection service stopped or started.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>Deep packet inspector state change alert</td>
<td>306-50008</td>
<td>Deep packet inspection engine on IPS or ADM stopped or started.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>Delete remote command</td>
<td>306-61</td>
<td>Alarm remote command removed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Deleted events</td>
<td>306-74</td>
<td>User deleted ESM events.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Deleted flows</td>
<td>306-75</td>
<td>User deleted ESM flows.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Device add</td>
<td>306-18</td>
<td>New device added to the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Device delete</td>
<td>306-19</td>
<td>Existing device deleted from the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Device possibly down</td>
<td>146-2</td>
<td>Network discovery event stating a device. can be down.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Device unreachable</td>
<td>146-1</td>
<td>Network discovery device added to ESM is unreachable.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Disk drive failure alert</td>
<td>306-50018</td>
<td>Checks and verifies integrity of all hard disks (internal or DAS).</td>
<td>Hardware Monitor</td>
<td>All</td>
<td>High</td>
</tr>
<tr>
<td>ELM archive process state change alert</td>
<td>306-50045</td>
<td>ELM compressing engine stopped or started.</td>
<td>Software Monitor</td>
<td>APM/REC/IPS/DBM</td>
<td>Medium</td>
</tr>
<tr>
<td>ELM EDS FTP</td>
<td>306-50074</td>
<td>ELM SFTP program stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>Medium</td>
</tr>
<tr>
<td>ELM file process</td>
<td>306-50065</td>
<td>ELM reininsertion engine stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>Medium</td>
</tr>
<tr>
<td>ELM FTI alert</td>
<td>306-50064</td>
<td>ELM Full Text Indexing engine stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>Medium</td>
</tr>
<tr>
<td>ELM mount point state change alert</td>
<td>306-50053</td>
<td>ELM remote storage (CIFS, NFS, ISCSI, SAN) stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>Medium</td>
</tr>
<tr>
<td>Rule name</td>
<td>Signature ID</td>
<td>Description</td>
<td>Type</td>
<td>Device</td>
<td>Severity</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------</td>
</tr>
<tr>
<td>ELM query engine state change alert</td>
<td>306-50046</td>
<td>ELM Jobs process - all ELM jobs, such as ELM queries and inserts, stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>Medium</td>
</tr>
<tr>
<td>ELM redundant storage</td>
<td>306-50063</td>
<td>ELM Mirror stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>Medium</td>
</tr>
<tr>
<td>ELM system database error</td>
<td>306-50044</td>
<td>ELM database stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>High</td>
</tr>
<tr>
<td>Email collector state change alert</td>
<td>306-50040</td>
<td>Cisco MARS collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>EPO tags applied</td>
<td>306-28</td>
<td>McAfee ePO tags applied.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Error communicating with ELM</td>
<td>306-50047</td>
<td>Communication with ELM failed.</td>
<td>Software Monitor</td>
<td>APM/REC/ IPS/DBM</td>
<td>High</td>
</tr>
<tr>
<td>Error in SSH communication</td>
<td>306-50077</td>
<td>Device issues communicating with the ELM (such as, version difference, change in key).</td>
<td>Software Monitor</td>
<td>All</td>
<td>High</td>
</tr>
<tr>
<td>ESM reboot</td>
<td>306-32</td>
<td>ESM rebooted.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>ESM shutdown</td>
<td>306-33</td>
<td>ESM shut down.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>eStreamer Collector alert</td>
<td>306-50070</td>
<td>eStreamer collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>eStreamer Collector state change alert</td>
<td>306-50041</td>
<td>eStreamer collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Event partition detach</td>
<td>306-4</td>
<td>Event partition detached.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Execute remote command</td>
<td>306-62</td>
<td>Alarm remote command executed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Failed login due to maximum concurrent sessions reached</td>
<td>306-37</td>
<td>User failed to log on because the maximum concurrent sessions were reached.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>Failed to format SAN device</td>
<td>306-50057</td>
<td>SAN on ELM failed to format; user must retry.</td>
<td>Hardware Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>Failed user login</td>
<td>306-31</td>
<td>User failed to log on.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>File collector state change alert</td>
<td>306-50049</td>
<td>Mount collector program stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>File deleted</td>
<td>306-50</td>
<td>Any file that can be added or removed, such as ESM log or sound file removed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Filter process state change alert</td>
<td>306-50050</td>
<td>Filter program on the device stopped or started (filter rules).</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Firewall alert aggregator state change alert</td>
<td>306-50009</td>
<td>Firewall aggregator on the IPS or ADM stopped or started.</td>
<td>Software Monitor</td>
<td>IPS/ADM/IP</td>
<td>Medium</td>
</tr>
<tr>
<td>Rule name</td>
<td>Signature ID</td>
<td>Description</td>
<td>Type</td>
<td>Device</td>
<td>Severity</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Flow partition detach</td>
<td>306-5</td>
<td>Flow partition detached.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Get VA data failure</td>
<td>306-52</td>
<td>ESM failed to obtain VA data.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>Get VA data success</td>
<td>306-51</td>
<td>ESM obtained VA data.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Health monitor internal alert</td>
<td>306-50027</td>
<td>Health Monitor process stopped or started.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>HTTP collector state change alert</td>
<td>306-50039</td>
<td>HTTP collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Indexing configuration change</td>
<td>306-8</td>
<td>ESM indexing settings changed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>Invalid SSH key</td>
<td>306-50075</td>
<td>Device issues communicating with ELM, such as version differences, change in key.</td>
<td>Software Monitor</td>
<td>All</td>
<td>High</td>
</tr>
<tr>
<td>IPFIX collector state change alert</td>
<td>306-50055</td>
<td>IPFIX (flow) collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Key &amp; certificate administrator user login</td>
<td>306-39</td>
<td>UCAPL event, Crypto admin logon.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Log partition rolled off</td>
<td>306-34</td>
<td>Oldest partitions for the database log table rolled off.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Log partitions free disk space alert</td>
<td>306-50004</td>
<td>Log partition (/var) is low on free space.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>McAfee EDB database server state change alert</td>
<td>306-50010</td>
<td>Database stopped or started.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>McAfee ePO Collector alert</td>
<td>306-50069</td>
<td>McAfee ePO collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>McAfee Event Format state change alert</td>
<td>306-50031</td>
<td>McAfee Event Format collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>McAfee SIEM device communication failure</td>
<td>306-26</td>
<td>ESM cannot communicate with another device.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>Microsoft Forefront Threat Management Gateway alert</td>
<td>306-50068</td>
<td>Forefront Threat Management Gateway collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>MS-SQL retriever state change alert</td>
<td>306-50035</td>
<td>MS SQL collector stopped or started (any data source for MS SQL).</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Multi-event log alert</td>
<td>306-50062</td>
<td>jEMAIL collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>MVM scan initiated</td>
<td>306-27</td>
<td>MVM scan started.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>NetFlow collector state change alert</td>
<td>306-50024</td>
<td>NetFlow (flow) collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Rule name</td>
<td>Signature ID</td>
<td>Description</td>
<td>Type</td>
<td>Device</td>
<td>Severity</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>New user account</td>
<td>306-13</td>
<td>New user added to the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>NFS/CIFS collector state change alert</td>
<td>306-50048</td>
<td>Remote mount for NFS or CIFS stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>NitroFlow collector state change alert</td>
<td>306-50026</td>
<td>NitroFlow (flows on device) stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>No SSH key found</td>
<td>306-50076</td>
<td>Device issues communicating with the ELM, such as version differences, change in key.</td>
<td>Software Monitor</td>
<td>All</td>
<td>High</td>
</tr>
<tr>
<td>NSM add/edit Blacklist</td>
<td>306-29</td>
<td>NSM Blacklist entry added or edited.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>NSM delete Blacklist</td>
<td>306-30</td>
<td>NSM Blacklist entry deleted.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>OPSEC retriever state change alert</td>
<td>306-50028</td>
<td>OPSEC (Check Point) collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>OPSEC retriever state change alert</td>
<td>306-50034</td>
<td>OPSEC (Check Point) collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Oracle IDM Collector alert</td>
<td>306-50072</td>
<td>Oracle IDM Collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Oversubscription alert</td>
<td>306-50012</td>
<td>ADM or IPS entered or exited oversubscription mode.</td>
<td>Software Monitor</td>
<td>IPS/ADM/IPS</td>
<td>Medium</td>
</tr>
<tr>
<td>Plug-in Collector/Parser alert</td>
<td>306-50073</td>
<td>Plug-in collector/parser stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Policy add</td>
<td>306-15</td>
<td>Policy added to the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Policy delete</td>
<td>306-17</td>
<td>Policy deleted from the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Policy modify</td>
<td>306-16</td>
<td>Policy changed in the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Previous configuration mismatch</td>
<td>146-6</td>
<td>Network discovery device configuration changed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Receiver HA</td>
<td>306-50058</td>
<td>Any HA process stopped or started (Corosync, HA Control script).</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Receiver HA Opsec configuration</td>
<td>306-50059</td>
<td>Not in use.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Low</td>
</tr>
<tr>
<td>Redundant ESM out of sync</td>
<td>306-76</td>
<td>Redundant ESM out of sync.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>High</td>
</tr>
<tr>
<td>Remote NFS mount point state change alert</td>
<td>306-50020</td>
<td>NFS ELM mount stopped or started.</td>
<td>Software Monitor</td>
<td>ELM</td>
<td>Medium</td>
</tr>
<tr>
<td>Remote share/mount point free disk space alert</td>
<td>306-50021</td>
<td>Free space on remote mount point is low.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>Rule name</td>
<td>Signature ID</td>
<td>Description</td>
<td>Type</td>
<td>Device</td>
<td>Severity</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Remote SMB/CIFS share state change alert</td>
<td>306-50019</td>
<td>Remote SMB/CIFS mount point stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Risk Correlation state change alert</td>
<td>306-50061</td>
<td>Risk Correlation engine stopped or started.</td>
<td>Software Monitor</td>
<td>ACE</td>
<td>Medium</td>
</tr>
<tr>
<td>Root partitions free disk space alert</td>
<td>307-50002</td>
<td>Free space on the root partitions is low.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>Rule add</td>
<td>306-20</td>
<td>Rule added to the system, such as ASP, filter, or correlation.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Rule delete</td>
<td>306-22</td>
<td>Rule deleted from the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Rule modify</td>
<td>306-21</td>
<td>Rule changed in the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Rule update failure</td>
<td>306-9</td>
<td>ESM rule update failed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Medium</td>
</tr>
<tr>
<td>SDEE retriever state change alert</td>
<td>306-50033</td>
<td>SDEE collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>sFlow collector state change alert</td>
<td>306-50025</td>
<td>sFlow (flow) collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>SNMP collector state change alert</td>
<td>306-50023</td>
<td>SNMP collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>SQL collector state change alert</td>
<td>306-50038</td>
<td>SQL collector (old NFX) stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Symantec AV collector state change alert</td>
<td>306-50056</td>
<td>Symantec AV collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>Syslog Collector state change alert</td>
<td>306-50037</td>
<td>Syslog collector stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>System admin user login</td>
<td>306-40</td>
<td>System administrator logged on to the system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>System integrity check failure</td>
<td>306-50085</td>
<td>Non-ISO foreign program or process running on the system is flagged.</td>
<td>Software Monitor</td>
<td>All</td>
<td>High</td>
</tr>
<tr>
<td>System logger state change alert</td>
<td>306-50014</td>
<td>System logging process stopped or started.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>Task (query) terminated</td>
<td>306-54</td>
<td>Task manager task closed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>Temporary partitions free disk space alert</td>
<td>306-50003</td>
<td>Temporary (/tmp) partition low on disk space.</td>
<td>Software Monitor</td>
<td>All</td>
<td>Medium</td>
</tr>
<tr>
<td>Text log parser state change alert</td>
<td>306-50052</td>
<td>Textparser process stopped or started.</td>
<td>Software Monitor</td>
<td>Receiver</td>
<td>Medium</td>
</tr>
<tr>
<td>User account change</td>
<td>306-14</td>
<td>User account changed.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>User device failed login</td>
<td>306-50079</td>
<td>SSH user failed to log on.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
<tr>
<td>User device login</td>
<td>306-50017</td>
<td>Not used in system.</td>
<td>Software Monitor</td>
<td>ESM</td>
<td>Low</td>
</tr>
</tbody>
</table>
## Copy an alarm

You can use an existing alarm as a template for a new alarm by copying and saving it with a different name.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Alarms**.
2. Select the alarm you want to copy, then click **Copy**.
   
   The **Alarm Name** page displays the name of the current alarm followed by _copy.

3. Change the name, then click **OK**.
4. To make changes to the alarm settings, select the copied alarm and click **Edit**.
5. Change the settings as needed.

**See also**

*Create an alarm on page 200*

---

### Enable or disable alarm monitoring

Alarm monitoring is enabled by default. You can disable it, then re-enable it as needed.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Alarms**.
2. Click the **Settings** tab, then click **Disable**.
   
   Alarm monitoring stops and the button changes to **Enable**.
3. Click **Enable** to resume monitoring 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.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, then click the **Properties** icon.
2. On the **System Properties** page, click **Alarms**, then click **Add**.
3. On the **Condition** tab, select the **Field Match** or **Internal Event Match** type.
4. Click the **Actions** tab, click **Create a case for**, click the variables icon, then select the fields to include in the case summary.
5. Click **Customize triggered alarm summary**, click the variables icon, then select the fields to include in the summary for the triggered alarm.
6. Type the other information requested to set up the alarm (see **Create an alarm**), then click **Finish**.

---

**Manage alarm message templates**

One of the actions available when setting up an alarm is **Send Message**. This allows you to forward alarm information to email or selected Short Message Services (SMS), SNMP, or Syslog recipients. You can add templates to define the information that you want in these messages, designing them to include what is most useful to the recipient. You can then select the template when you define the action for an alarm.

You can add templates to define the information that you want in these messages, designing them to include what is most useful to the recipient. You can then select the template when you define the action for an alarm.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Alarms**.
2. Click the **Settings** tab, then click **Templates**.
3. View the list of existing templates or select any of the available options, then click **OK**.
Manage alarm audio files
You can upload and download audio files to use them for audio alerts.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Alarms.
2. Click the Settings tab, then click Audio.
3. Download, upload, remove, or play audio files, then click Close.

Manage alarm recipients
When you are defining the action settings for an alarm, you can send a message to recipients. You can manage the recipients lists from the Alarms page.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Alarms.
2. Click the Settings tab, then click Recipients.
3. Select the type of recipients list you want to manage, then add, edit, or remove recipients.

Manage alarms
When an alarm is triggered, you can acknowledge it, delete it, or view the details. You can also unacknowledge an alarm, change the assignee, and create a case from an alarm.

**Task**
For option definitions, click ? in the interface.

1. Access one of these:
   - Alarm log pane — Located below the system navigation tree.
   - Visual pop-up alert — Opens when an alarm triggers.
   - Details page — Opens when you click the Details icon on the Alarms log pane.
2 Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acknowledge an alarm</td>
<td>Click the <strong>Acknowledge</strong> icon.</td>
</tr>
<tr>
<td>Unacknowledge an alarm</td>
<td>Click the <strong>Unacknowledge</strong> icon.</td>
</tr>
<tr>
<td>Delete an alarm</td>
<td>Click the <strong>Delete</strong> icon.</td>
</tr>
<tr>
<td>View alarm details</td>
<td>On the <strong>Alarms</strong> log pane or visual pop-up alert, click the <strong>Details</strong> icon.</td>
</tr>
<tr>
<td>Change assignee</td>
<td>On the <strong>Details</strong> page, click <strong>Assignee</strong> and select a name.</td>
</tr>
<tr>
<td>Create a case from an alarm</td>
<td>On the <strong>Details</strong> page, click <strong>Create Case</strong>.</td>
</tr>
</tbody>
</table>

**Tasks**

- **View alarm reports queue on page 216**
  If you selected **Generate reports** as the action for an alarm, you can view or make changes to the reports that are waiting to run, and view the completed reports.

- **Manage alarm report files on page 216**
  After an alarm report runs, it's added to the list of available reports on the ESM. You can view this list and perform various actions.

**See also**

*Add a case on page 267*

**View alarm reports queue**

If you selected **Generate reports** as the action for an alarm, you can view or make changes to the reports that are waiting to run, and view the completed reports.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, click **Alarms**, then click the **Settings** tab.

2. Do one of the following:
   - To view or cancel reports queued to run, click **View**.
   - To view and manage completed reports, click **Files**.

3. Click **Close**.

**Manage alarm report files**

After an alarm report runs, it's added to the list of available reports on the ESM. You can view this list and perform various actions.
**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Alarms**.

2. Click the **Settings** tab, click **Files**, then select whether to download or remove reports from the list, or upload reports to this list.

3. Click **Close**.
Working with alarms
Manage alarms
Working with events

The ESM enables you to identify, collect, process, correlate, and store billions of events and flows, keeping all information available for queries, forensics, rules validation, and compliance.

Contents

- Events, flows, and logs
- Managing reports
- Description of contains and regex filters
- Working with ESM views
- Custom type filters

Events, flows, and logs

*Events, flows, and logs* record different types of activities that occur on a device.

An *event* is an activity recorded by a device as a result of a rule on your system. A *flow* is the record of a connection made between IPs, at least one of which is on your HOME_NET. A *log* is a record of an event that occurred to a device on your system. Events and flows have source and destination IP addresses, ports, Media Access Control (MAC) addresses, a protocol, and a first and last time (indicating the duration between the initiation of the connection to its termination). However, there are several differences between events and flows:

- Because flows are not an indication of anomalous or malicious traffic, they are more common than events.
- A flow is not associated with a rule signature (SigID) like an event is.
- Flows are not associated with event actions such as alert, drop, and reject.
- Certain data is unique to flows, including source and destination bytes, and source and destination packets. *Source bytes and packets* are the number of bytes and packets transmitted by the source of the flow, while the *destination bytes and packets* are the number of bytes and packets transmitted by the destination of the flow.
- Flows have direction: An *inbound flow* is defined as a flow that originates from outside of the HOME_NET. An *outbound flow* originates from outside the HOME_NET. This variable is defined in a policy for a Nitro IPS.
Events and flows generated by the system can be seen on views, which you can select on the views drop-down list. Logs are listed on the System Log or Device Log accessed from the Properties page for the system or each device.

**Set up events, flows, and logs downloads**
Check for events, flows, and logs manually or set the device to check for them automatically.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Events, Flows & Logs, Events & Logs, or Logs.
3. Set up the downloads, then click Apply.

**Limit time for data collection**
You can schedule a daily time range to limit when the ESM pulls data from each device and when data is sent to the ELM from each device.

**Before you begin**
Disable Dynamic Aggregation and set Level 1 Aggregation to between 240 and 360 minutes (see Change event or flow aggregation settings).

You can use this feature to avoid using the network at peak times, leaving the bandwidth available for other applications. This does delay data delivery to the ESM and ELM, so determine if this delay is acceptable in your environment.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select the device, then click the Properties icon.
2. Select one of the following:
   - Events, Flows & Logs
   - Events & Logs
   - Logs
3. Select Define daily data pull time range, then set the start time and end time for the time range.

The ESM collects data from the device and the device sends data to the ELM for logging during the time range you defined. When you set this up on an ELM, it defines when the ESM collects data from the ELM and when the ESM sends data to the ELM for logging.

**Define inactivity threshold settings**
When you set an inactivity threshold for a device, you are notified when no events or flows are generated in the specified period of time. If the threshold is reached, a yellow health status flag appears next to the device node on the system navigation tree.
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, make sure that System Information is selected, then click Events, Flows, & Logs.
2. Click Inactivity Settings.
3. Highlight the device, then click Edit.
4. Make changes to the settings, then click OK.

**Get events and flows**
Retrieve events and flows for the devices you select on the system navigation tree.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, a group, or a device.
2. Click the Get Events and Flows icon on the actions toolbar, then follow the required steps.
3. Once the download is complete, select a view to display these events and flows on, then click the Refresh Current View icon on the views toolbar.

**Check for events, flows, and logs**
You can set the ESM to check for events, flows, and logs automatically or you can check for them manually. The rate at which you check for them depends on your system’s level of activity and how often you want to receive status updates. You can also specify which devices should check for each type of information and set the inactivity threshold settings for the devices managed by the ESM.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Events, Flows, & Logs.
2. Make the selections and changes for event, flow, and log retrieval.
3. Click OK.

**See also**
*Define inactivity threshold settings on page 220*

**Define geolocation and ASN settings**
Geolocation provides the real-world geographic location of computers connected to the Internet. Autonomous System Number (ASN) is a number that is assigned to an autonomous system and uniquely identifies each network on the Internet. Both of these types of data can help you identify the physical location of a threat. Source and destination geolocation data can be collected for events.
Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Events, Flows & Logs or Events & Logs, then click Geolocation.
3. Make the selections to generate the information needed, then click OK.

You can filter event data using this information.

Get events and flows
Retrieve events and flows for the devices you select on the system navigation tree.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, a group, or a device.
2. Click the Get Events and Flows icon on the actions toolbar, then follow the required steps.
3. Once the download is complete, select a view to display these events and flows on, then click the Refresh Current View icon on the views toolbar.

Aggregating events or flows
An event or flow can potentially be generated thousands of times. Instead of forcing you to sift through thousands of identical events, aggregation allows you to view them as a single event or flow with a count that indicates the number of times it occurred.

Using aggregation uses disk space on both the device and ESM more efficiently because it eliminates the need to store each packet. This feature applies only to rules that have aggregation enabled in the Policy Editor.

Source IP and destination IP address
The source IP 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: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 ten minutes after noon, the First time field contains the time 12:00 (the time of the first instance of the event), the Last time field contains the time 12:10 (the time of the last instance of the event), and the Total field contains the value 30.

You can change the default event or flow aggregation settings for the device as a whole and, for events, you can add exceptions to the device's settings for individual rules (see Manage event aggregation exceptions).
Dynamic aggregation is also enabled by default. When it is selected, it replaces the settings for Level 1 aggregation and increases the settings for Level 2 and Level 3. It 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 that it is pulled by the ESM. 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 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 privileges to change these settings.

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

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Event Aggregation or Flow Aggregation.
3. Define the settings, then click OK.

**Add exceptions to event aggregation settings**

Aggregation settings apply to all events generated by a device. You can create exceptions for individual rules if the general settings don't apply to the events generated by that rule.

**Task**

For option definitions, click ? in the interface.

1. On the views pane, select an event generated by the rule you want to add an exception for.
2. Click the Menu icon, then select Modify Aggregation Settings.
3. Select the field types you want to aggregate from the Field 2 and Field 3 drop-down lists.

The fields you select in Field 2 and Field 3 must be different types or an error results. When you select these field types, the description for each aggregation level changes to reflect the selections you made. The time limits for each level depend on the event aggregation setting you defined for the device.

4. Click OK to save your settings, then click Yes to proceed.
5. Deselect devices if you do not want to roll out the changes to them.
6. Click OK to roll out the changes to the devices that are selected.

The Status column shows the status of the update as the changes are rolled out.
Manage event aggregation exceptions
You can view a list of the event aggregation exceptions that were added to the system. You can also edit or remove an exception.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device, then click the Properties icon.
2. Click Event Aggregation, then click View at the bottom of the screen.
3. Make the needed changes, then click Close.

Setting up event forwarding
Event forwarding allows you to send events from the ESM to another device or facility by Syslog or SNMP (if enabled). You must define the destination, and can select if you want to include the packet and obfuscate the IP data. You can add filters so the event data is filtered before it is forwarded. This isn't a substitute for log management, because it's not a full set of digitally signed logs from each device in your environment.

Configure event forwarding
You can set up an event forwarding destination to forward event data to a syslog or SNMP server.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Event Forwarding.
2. On the Event Forwarding Destinations page, select Add, Edit, or Remove.
3. If you selected to add or edit a destination, define the settings.
4. Click Apply or OK.

Add event forwarding destinations
Add an event forwarding destination to the ESM to forward event data to a syslog or SNMP server.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Event Forwarding.
2. Click Add, then fill in the requested information.
3. Click OK.

See also
Event forwarding agents on page 225
### Event forwarding agents

These are the event forwarding agents and the information contained within the packets when they are forwarded. You select the agent in the Format field on the Add Event Forwarding Destination page.

<table>
<thead>
<tr>
<th>Agent</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syslog</td>
<td>ESM IP McAfee ESM (part of syslog header), SigID, SigMessage, SrcIP, DstIP, SrcPort, DstPort, SrcMac, DstMac, Protocol, VLAN, Flow (whether the event is generated by the initiator of the connection or the recipient of the connection), EventCount, FirstTime (in UNIX time format), LastTime (in UNIX time format), LastTime_usec, Event Subtype, Severity, InternalID (event ID on the ESM), EventID, IPSID, IPSName (datasource name : IP address), DSID (Datasource ID), Source IPv6, Dest IPv6, Session ID, Sequence, Trusted flag, Normalized ID, GUID Source, GUID Dest, Agg 1 Name, Agg 1 Value, Agg 2 Name, Agg 2 Value, Agg 3 Name, Agg 3 Value. The following string fields are also in quotes because they might contain a semicolon: Application, Command, Domain, Host, Object, Destination User, Source User, User-defined type 8, User-defined type 9, User-defined type 10, User-defined type 21, User-defined type 22, User-defined type 23, User-defined type 24, User-defined type 25, User-defined type 26, User-defined type 27. Packet (packet contents follow Base 64 encoding only if the &quot;copy packet&quot; option is &quot;on&quot; for the rules in the policy editor and the option is checked while setting up event forwarding on the ESM).</td>
</tr>
<tr>
<td>Syslog</td>
<td>ESM IP McAfee ESM (part of syslog header), SigID, SigMessage, SrcIP, DstIP, SrcPort, DstPort, SrcMac, DstMac, Protocol, VLAN, Flow (whether the event is generated by the initiator of the connection or the recipient of the connection), EventCount, FirstTime (in UNIX time format), LastTime (in UNIX time format), LastTime_usec, Event Subtype, Severity, InternalID (event ID on the ESM), EventID, IPSID, IPSName (datasource name : IP address), DSID (Datasource ID), Source IPv6, Dest IPv6, Session ID, Sequence, Trusted flag, Normalized ID. The following string fields are also in quotes because they might contain a semicolon: Application, Command, Domain, Host, Object, Destination User, Source User, User-defined type 8, User-defined type 9, User-defined type 10. Packet (packet contents follow Base 64 encoding only if the &quot;copy packet&quot; option is &quot;on&quot; for the rules in the policy editor and the option is checked while setting up event forwarding on the ESM).</td>
</tr>
<tr>
<td>Syslog</td>
<td>ESM IP, &quot;McAfee ESM,&quot; SigID, SigMessage, SrcIP, DstIP, SrcPort, DstPort, SrcMac, DstMac, Protocol, VLAN, Flow (whether the event is generated by the initiator of the connection or the recipient of the connection), EventCount, FirstTime (in UNIX time format), LastTime (in UNIX time format), LastTime_usec, Event Subtype, Severity, InternalID (event ID on the ESM), event ID, IPSID, IPSName, DSID (Datasource ID), Packet (packet contents follow Base 64 encoding).</td>
</tr>
<tr>
<td>Syslog</td>
<td>&quot;McAfee,&quot; MachineID, &quot;ArcSite Notification,&quot; &quot;Line 1,&quot; Group Name, IPS Name, LastTime mm/dd/yyyy HH:mm:ss, LastTime_usec, FirstTime mm/dd/yyyy HH:mm:ss, SigID, Class Name, Event Count, Src IP, Src Port, Dst IP, Dst Port, Protocol, Event Subtype, Event Device ID (internal id for the event from the device), Event ESM ID (internal id for the event from the ESM), Rule Message, Flow (whether the event is generated by the initiator of the connection or the recipient of the connection), VLAN, Src MAC, Dst MAC, Packet (packet contents follow Base 64 encoding).</td>
</tr>
<tr>
<td>Syslog</td>
<td>snort:, [sigid:smallsigid:0], Signature Message or &quot;Alert,&quot; [Classification: ClassName], [Priority: ClassPriority], {Protocol}, SrcIP:SrcPort -&gt; DstIP:DstPort, SrcIP -&gt; DstIP, Packet (packet contents follow Base 64 encoding).</td>
</tr>
<tr>
<td>Syslog</td>
<td>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.</td>
</tr>
</tbody>
</table>
Enable or disable event forwarding

Enable or disable event forwarding on the ESM.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
2. Click **Settings**, then select or deselect **Event Forwarding Enabled**.
3. Click **OK**.

Modify settings for all event forwarding destinations

Change some settings for all existing event forwarding destinations at one time.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
2. Click **Settings**, then set the options.
3. Click **OK**.

Add event forwarding filters

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

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Event Forwarding**.
2. Click **Add**, then click **Event Filters**.
3. Fill in the filter fields, then click **OK**.
Edit event forwarding filter settings

Change filter settings for event forwarding after they are saved.

**Before you begin**

When editing a device filter, you must have access to all the devices in the filter. To enable access to the devices, see *Set up user groups*.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select *System Properties*, then click *Event Forwarding*.
2. Click *Edit*, then click *Event Filters*.
3. Make the changes, then click *OK*.

**See also**

*Set up user groups on page 177*

**Sending and forwarding events with Standard Event Format**

Standard Event Format (SEF) is a Java Script Object Notation (JSON)-based event format to represent generic event data.

SEF format forwards events from the ESM to a Receiver on a different ESM, as well as from the ESM to a third party. You can also use it to send events from a third party to a Receiver by selecting SEF as the data format when creating the data source.

When setting up event forwarding with SEF from ESM to ESM, you need to perform four steps:

1. Export data sources, custom types, and custom rules from the ESM that is forwarding the events.
   - To export the data sources, follow the instructions in *Move data sources to another system*.
   - To export the custom types, open *System Properties*, click *Custom Types*, then click *Export*.
   - To export the custom rules, follow the instructions in *Export rules*.

2. On the ESM with the Receiver you are forwarding to, import the data sources, custom types, and custom rules that you just exported.
   - To import the data sources, follow the instructions in *Move data sources to another system*.
   - To import the custom types, open *System Properties*, click *Custom Types*, then click *Import*.
   - To import the custom rules, follow the instructions in *Import rules*. 
3 On the ESM that is receiving the events from another ESM, add an ESM data source.
   — On the system navigation tree, click the Receiver device you want to add the data source to, then click the Add Data Source icon.
   — On the Add Data Source page, select McAfee in the Data Source Vendor field, then Enterprise Security Manager (SEF) in the Data Source Model field.
   — Complete the requested information, then click OK.

4 Add the event forwarding destination on the sending ESM.
   — Click the system on the system navigation tree, then click the Properties icon.
   — Click Event Forwarding, then click Add.
   — On the Add Event Forwarding Destination page, select syslog (Standard Event Format) in the Format field, then complete the remaining fields with the information for the ESM you are forwarding to, and click OK.

Managing reports
Reports show data from events and flows managed on the ESM. You can design your own or run one of the predefined reports and send it in PDF, HTML, or CSV format.

Predefined reports
The predefined reports are divided into these categories:
- Compliance
- Executive
- McAfee ADM
- McAfee Database Activity Monitoring (DAM)
- McAfee DEM
- McAfee Event Reporter

They generate data based on events.

User-defined reports
When you create a report, you design the layout on the Report Layout editor by selecting the orientation, size, font, margins, and header and footer. You can also include components, setting them up to display the data as desired.

All layouts are saved and can be used for multiple reports. When you add a report, you are given the option to design a new layout, use an existing one as is, or use an existing one as a template and edit its features. You can also remove a report layout when it is no longer needed.

See also
Add a report condition on page 230
Set start month for quarterly reports on page 228
Add report layout on page 229

Set start month for quarterly reports
If you are running reports on a quarterly basis, you must define the first month of Quarter 1. Once this is defined and stored in the system table, reports run quarterly based on that start date.
Task
For option definitions, click ? in the interface.

1. On the ESM console, select System Properties, then click Custom Settings.
2. In the Specify which month should be used field, select the month.
3. Click Apply to save the setting.

Add a report
Add reports to the ESM and set them to run on a regular basis, at intervals you define, or run when you select them manually. You can select an existing report layout or create a new one using the Report Layout editor.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Reports.
2. Click Add, then define the settings on the Add Report page.
3. Click Save.

The report is added to the table on the Reports page and runs as defined in the Condition field.

Add report layout
Design the layout for a report if the predefined layouts do not meet your needs.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Reports.
2. Click Add to open the Add Report page, then complete sections 1, 2, and 3.
3. In section 4, select Report PDF or Report HTML.
4. In section 5, click Add to open the Report Layout editor.
5. Set up the layout to display the data generated by the report.

The layout is saved and can be used as is for other reports or as a template that you can edit.

Include an image in PDFs and reports
You can set up the ESM so exported PDFs and printed reports include the image shown on the Login screen.

Before you begin
Add the image to the Custom Settings page (see Customize the login page).
**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Custom Settings.
2. Select Include image in exported PDF from Views or printed reports.
3. Click OK.

**See also**
Customize the logon page on page 20

**Add a report condition**
Add conditions so they are available when setting up a report.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select System Properties, then click Reports.
2. Click Conditions, then enter the information requested.
3. Click OK to save the settings.

This option appears on the list of available conditions when you select the condition for a report.

**Display host names in a report**
You can configure reports to use DNS resolution for source and destination IP addresses on reports.

**Task**
For option definitions, click ? in the interface.

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).

**Description of contains and regex filters**
The contains and regex filters provide you with wildcard capabilities on both index string data and non-indexed string data. These filters have syntax requirements.

These commands can be used in any field that allows text or string data. Most text fields are denoted by the case insensitivity icon next to the filter field name. Other fields that allow contains do not have that icon. For a full list of fields, see the Fields supporting the contains feature section.
Syntax and Examples

The basic syntax for contains is contains(somevalue) and for regex is regex(someregularexpression).

To make it case insensitive, click the case insensitive icon or include the /i regular expression notation, as in regex(/somevalue/i). The search returns any value that contains somevalue, regardless of case.

The NOT and OR icons apply to the regex and contains values. If you want the results to show the values that do not contain some value, enter the value and click the NOT icon. If you want the results to show values that have one value or another, enter the values and click the OR icon.

Example #1 - A simple search

Indexed fields: contains(stra), regex(stra)
Non-indexed fields: stra
Result: Returns any string with stra, such as administrator, gmestrad, or straub.

Example #2 - An OR search

Indexed fields: contains(admin,NGCP), regex((admin|NGCP))
Non-indexed fields: admin, NGCP
Results: Returns any string within the field that contains admin or NGCP. The extra set of parentheses is required for the regex OR to function.

Example #3 - A search for special characters, such as in service accounts

A dollar sign:

Indexed fields: contains($), regex(\x24) or regex(\$)
Non-indexed fields: $
Results: Either of these returns any string within the field that contains a $. Go to http://www.ascii.cl for a list of HEX values for the characters.

With regex, if you try to use the $ without scaling it, the result set returns empty. PCRE escape sequence is a better search method to use.

A percent sign:

Indexed fields: contains(%), regex(\x25) or regex(\%)
Non-indexed fields: 

A backslash:

Indexed fields: contains(\), regex(\x5c) or regex(\\)
Non-indexed fields: 

Dual back slashes
Indexed fields: `contains(\), regex(\x[0-9a-f]{2}\x) or regex(\)\)

Non-indexed fields: \}

In some cases, if you do not use the HEX value or the slash with regex, you may get an Invalid Regular Expression (ER5-0015) error.

Example #4 - Search using the * wildcard

Indexed fields: `contains (ad*)`

Non-indexed fields: ad*

Results: Returns any string that starts with ad, such as administrator and address.

Example #5 - Search using Regular Expression

`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)

These domains are from Microsoft DNS events.

Results: This regular expression picks out a specific string. In this case, it's nitroguard, a 3- or 4-digit primary domain, and com or info. This regex matches the first two expressions but not the others. These are examples to show how regex can be used with the feature. Your expressions will be much different.

Caveats

- Using regex with values of less than three characters causes higher overhead and slower query performance. We suggest that all queries have more than three characters.

- This filter can't be used in correlation rules or alarms. The only exception is that it can be used in correlation rules with name/value custom types.

- Using contains or regex with NOT can cause higher overhead and slower query performance.

Bloom filter description

For information regarding a bloom filter, see http://en.wikipedia.org/wiki/Bloom_filter

Fields supporting the `contains` and `regex` feature

<table>
<thead>
<tr>
<th>Access_Resource</th>
<th>File_Operation_Succeeded</th>
<th>Referer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>File_Type</td>
<td>Registry_Key</td>
</tr>
<tr>
<td>Application_Protocol</td>
<td>Registry_Value</td>
<td></td>
</tr>
<tr>
<td>Area</td>
<td>Filename</td>
<td>Request_Type</td>
</tr>
<tr>
<td>Authoritative_Answer</td>
<td>Forwarding_Status</td>
<td>Response_Code</td>
</tr>
<tr>
<td>Bcc</td>
<td>From</td>
<td>Return_Code</td>
</tr>
<tr>
<td>Column Name</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>Caller_Process</td>
<td>From_Address</td>
<td></td>
</tr>
<tr>
<td>Catalog_Name</td>
<td>FTP_Command</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Host</td>
<td></td>
</tr>
<tr>
<td>Cc</td>
<td>HTTP_Request_Cookie</td>
<td></td>
</tr>
<tr>
<td>Client_Version</td>
<td>HTTP_Request_Host</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>HTTP_Request_Method</td>
<td></td>
</tr>
<tr>
<td>Contact_Name</td>
<td>HTTP_Request_Sender</td>
<td></td>
</tr>
<tr>
<td>Contact_Nickname</td>
<td>HTTP_Request_URL</td>
<td></td>
</tr>
<tr>
<td>Cookie</td>
<td>HTTP_User_Agent</td>
<td></td>
</tr>
<tr>
<td>Creator_Name</td>
<td>Incomting_ID</td>
<td></td>
</tr>
<tr>
<td>Database_ID</td>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>Database_Name</td>
<td>Interface_Dest</td>
<td></td>
</tr>
<tr>
<td>Datacenter_ID</td>
<td>Job_Name</td>
<td></td>
</tr>
<tr>
<td>Datacenter_Name</td>
<td>Job_Type</td>
<td></td>
</tr>
<tr>
<td>DB2_Plan_Name</td>
<td>Language</td>
<td></td>
</tr>
<tr>
<td>Delivery_ID</td>
<td>Local_User_Name</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>Logical_Unit_Name</td>
<td></td>
</tr>
<tr>
<td>Destination_User</td>
<td>Logon_Type</td>
<td></td>
</tr>
<tr>
<td>Destination_Directory</td>
<td>LPAR_DB2_Subsystem</td>
<td></td>
</tr>
<tr>
<td>Destination_Filename</td>
<td>Mail_ID</td>
<td></td>
</tr>
<tr>
<td>Destination_Hostname</td>
<td>Mailbox</td>
<td></td>
</tr>
<tr>
<td>Destination_Logo_ID</td>
<td>Mainframe_Job_Name</td>
<td></td>
</tr>
<tr>
<td>Destination_Network</td>
<td>Malware_Insp_Action</td>
<td></td>
</tr>
<tr>
<td>Destination_UserID</td>
<td>Malware_Insp_Result</td>
<td></td>
</tr>
<tr>
<td>Detection_Method</td>
<td>Management_Server</td>
<td></td>
</tr>
<tr>
<td>Device_Action</td>
<td>Message_ID</td>
<td></td>
</tr>
<tr>
<td>Direction</td>
<td>Message_Text</td>
<td></td>
</tr>
<tr>
<td>Directory</td>
<td>Method</td>
<td></td>
</tr>
<tr>
<td>DNS_Class</td>
<td>NTP_Client_Mode</td>
<td></td>
</tr>
<tr>
<td>DNS_Name</td>
<td>NTP_Opcode</td>
<td></td>
</tr>
<tr>
<td>DNS_Type</td>
<td>NTP_Request</td>
<td></td>
</tr>
<tr>
<td>Domain</td>
<td>NTP_Server_Mode</td>
<td></td>
</tr>
<tr>
<td>Event_Class</td>
<td>Object</td>
<td></td>
</tr>
<tr>
<td>External_Application</td>
<td>Object_Type</td>
<td></td>
</tr>
<tr>
<td>External_DB2_Server</td>
<td>Operating_System</td>
<td></td>
</tr>
<tr>
<td>External_Hostname</td>
<td>Policy_Name</td>
<td></td>
</tr>
<tr>
<td>External_SessionID</td>
<td>Privileged_User</td>
<td></td>
</tr>
<tr>
<td>Facility</td>
<td>Process_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Query_Response</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RTMP_Application</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sensor_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sensor_Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sensor_UUID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Session_Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signature_ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Signature_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP_Error_Code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP_Item</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP_Item_Type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP_Operation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SNMP_Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source_User</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source_Context</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source_Logon_ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source_Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source_User_ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Source_Zone</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL_Command</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL_Statement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Step_Count</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Step_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SWF_URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Table_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target_Context</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target_Doc-Class</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Target_Process_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TC_URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat_Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat_Handled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat_Name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To_Address</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>URL_Category</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User_Agent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User_Nickname</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Version</td>
<td></td>
</tr>
</tbody>
</table>
Working with ESM views

The ESM retrieves information about events, flows, assets, and vulnerabilities logged by a device. The information is correlated and inserted into the McAfee Security Event Aggregation and Correlation (MSEAC) engine.

Contents
- Using ESM views
- View session details
- Views toolbar
- Predefined views
- Add a custom view
- View components
- Working with the Query Wizard
- Manage views
- Look around an event
- View the IP address details of an event
- Change the default view
- Filtering views
- Watchlists
- String normalization

Using ESM views

Using the MSEAC engine, the data retrieved by the ESM can be analyzed and reviewed through a powerful and flexible report viewer. This viewer is the center section of the ESM console. The view shows the data for the devices you have selected on the system navigation tree.

When the ESM console is launched, the default view appears (see Change the default view). You can use the view features to select another predefined view (see Predefined views) or create a new view (see Add a custom view) to run a query so you can see what is occurring on your network (see ESM views toolbar). You can also use the various options on the views toolbar, component menu, and component toolbar to interact with the views and their data.

A progress bar is visible in each component of the views pane when a query is run. If you pass the cursor over it, it shows the amount and percentage of time that has elapsed in the execution of each component’s query. To cancel a query to free up ESM resources, click the delete icon to the right of the progress bar.

These custom types can use contains and regex:

Views
- String
- Random string
- Name/value
- Hashed strings

Case management
- Notes
- Summary
- History
On a view, source IP 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:FFFF:A00:C07 (A00:C07 is 10.0.12.7); ::0000:10.0.12.7 would be 10.0.12.7.

**View session details**

You can view the details of an event with a session ID and save them to a csv file on the Session Viewer.

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

**Task**

For option definitions, click ? in the interface.

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.

**Views toolbar**

The views toolbar, which is located at the top of the views pane, has several options you will use when setting up the views.

**Table 7-1**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 — Hide Device Tree</td>
<td>Click to expand the current view by hiding the device tree pane.</td>
</tr>
<tr>
<td>2 — View navigation</td>
<td>Navigate back and forth between previous views.</td>
</tr>
<tr>
<td>3 — View list</td>
<td>Select a view from the drop-down list, which lists all the predefined and custom views selected to display on this list.</td>
</tr>
<tr>
<td>4 — Manage views</td>
<td>Manage all the views (see Manage the views). You can select which views you want to include on the view list, add folders, and rename, delete, copy, import, and export views.</td>
</tr>
<tr>
<td>5 — Refresh current view</td>
<td>Refresh all data that is currently displayed in the view pane.</td>
</tr>
<tr>
<td>6 — Default view</td>
<td>Go back to default view.</td>
</tr>
</tbody>
</table>
Table 7-1

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 — Print current view</td>
<td>Print a copy of the current view. The print options are:</td>
</tr>
<tr>
<td></td>
<td>• Scale to fit all components on one page — The components that are part of the view are sized so the view fits on one page.</td>
</tr>
<tr>
<td></td>
<td>• Print each component on a separate page — Each component that is part of the view is printed on a separate page. If you click Scale component to fit page, each component is sized to fill the page.</td>
</tr>
<tr>
<td></td>
<td>• Print viewable area only — Only the portion of the view that is visible on the screen is printed.</td>
</tr>
<tr>
<td></td>
<td>• Export to PDF — The view is saved as a PDF file.</td>
</tr>
<tr>
<td>8 — Edit current view</td>
<td>Modify the view currently being displayed, if it is a custom view. Clicking this option opens the View Editing Toolbar (see Create a custom view).</td>
</tr>
<tr>
<td>9 — Create a new view</td>
<td>Create a new custom view (see Create a custom view).</td>
</tr>
<tr>
<td>10 — Timeframe</td>
<td>Specify the timeframe for the information that you want displayed in the view.</td>
</tr>
<tr>
<td>11 — Hide Filters</td>
<td>Click to expand the current view by hiding the filters pane.</td>
</tr>
</tbody>
</table>

Predefined views

The drop-down list on the views toolbar gives you access to the views that come with the system, as well as any custom views you add.

These are the different types of predefined views.

- **Asset, Threat & Risk** views summarize asset, threat, and risk data and their possible effects on your system.

- **Compliance Views** assist in streamlining regulation compliance activities.

- **Dashboard Views** provide an overview of specific aspects of the system.

- The **Device Status** view shows the status of the devices selected on the system navigation tree. If you click a device in the view, the health information for the selected device appears in the bottom half of the view.

- **Enhanced ELM Search** provides you with real-time tracking of the search progress and results. This view is available only if there is an ELM on the system (see Enhanced ELM Search View).

- **Event Views** break down the information generated by events associated with the device selected on the system navigation tree.
Executive Views provide an overview of aspects of the system that are of most interested to non-IT employees.

Flow Views break down the information recorded about each flow (or connection) made through the Nitro IPS (see Flow views).

McAfee Event Reporter includes product-specific views for many McAfee products.

Risk Views are used with the ACE default manager. To properly view data for custom managers, custom views must be built.

Event Workflow Views includes these views:
- Triggered Alarms – View and manage the alarms triggered when alarm conditions are met (see Triggered Alarms view).
- Case Management – View and manage the cases on the system (see View all cases).

Flow views
A flow is a record of a connection made through the device. When flow analysis is enabled on the Nitro IPS, data is recorded about each flow, or connection, made through the Nitro IPS.

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. This variable is defined in a policy for a Nitro IPS.

To view flow data, you must enable your system to log flow data. You can then view flows on the Flow Analysis view.

Enable flow logging
To view flow analysis data for a Nitro IPS, you must enable two firewall variables.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select a device.

2. Click the Policy Editor icon, then select Variable in the Rule Types pane.

3. Expand the Firewall category in the rule display pane.

4. On the INBOUND_CONNECTION_STATISTICS row, deselect Inherit to break the inherit value, then type Yes and click OK.

5. For OUTBOUND_CONNECTION_STATISTICS, deselect Inherit to break the inherit value, then type Yes and click OK.
Enhanced ELM search view

The Enhanced ELM Search view is available when there is at least one ELM device on the system. It allows you to perform more detailed searches and provides real-time tracking of search progress and results when you perform a search of logs on one or more ELM.

This view takes advantage of the archive statistical reporting capabilities on the ELM to provide real-time information about the amount of data that must be searched, allowing you to limit the query to minimize the number of files to be searched.

To enable faster search speeds when using Enhanced ELM Search, you must enable the full-text indexing engine, which increases the speed because it limits the number of files searched. For this increase to take effect, all existing ELM logs must be indexed. Once the indexer is enabled, indexing can take up to a few weeks, depending on the speed of the system and the number of logs that are collected. Search performance does not decrease during this time, but only improves as the ELM logs are indexed. To enable full-text indexing, see Enable faster ELM searches.

While the search is processing, the graphs show the estimated results:

- **Results Time Distribution** graph — Displays the estimates and results based on a time distribution. The bottom axis changes depending on what is selected in the time frame drop-down list.

- **Data Source Results** graph — Displays the estimates and results per data source based on the data sources of the devices selected on the system navigation tree.

- **Device Type Results** graph — Displays the estimates and results per device type based on the devices selected on the system navigation tree.

These graphs are populated before the searching begins and are updated as results are found. You can select one or more bars on the Data Source Results or Device Type Results graphs, or highlight a section of the Results Time Distribution graph. Click Apply Filters to narrow the search once the results have started coming in. This allows you to drill down to the search results, and to limit the amount of data that needs to be searched. When the search is finished, these graphs display the actual results.

Perform an enhanced ELM search

Search the logs on one or more ELM devices for information that you define. If the full text indexer is enabled, you can perform faster ELM searches because it limits the number of files that must be searched.

**Task**

For option definitions, click ? in the interface.

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.

   - This field doesn't support full-text indexing vocabulary, such as XOR and NOT. It does support AND and OR.

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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save search</td>
<td>Save the results of this search, even if you navigate away from the view. Saved searches can be viewed on the ELM Properties</td>
</tr>
<tr>
<td>Download search results file</td>
<td>Download the results to the location you designate.</td>
</tr>
<tr>
<td>Copy selected items to clipboard</td>
<td>Copy the items you select to the clipboard, so you can paste them into a document.</td>
</tr>
<tr>
<td>View data details</td>
<td>Show details for any logs that you select in the Search Results table.</td>
</tr>
</tbody>
</table>

**View and manage triggered alarms**

This view lists the triggered alarms and alarms that aren’t deleted. You can perform several actions to manage these alarms.

**Task**

For option definitions, click ? in the interface.

1 On the ESM console, select the quick launch **Alarms** icon to open the **Triggered Alarms** view.

2 Do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| 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 **Acknowledge Alarm** icon at the bottom of the view.  
                               | Acknowledged alarms are removed from the **Alarms** pane but remain on the **Triggered Alarms** view. |
| Delete an alarm from the system | • Select the triggered alarm that you want to delete, then click the **Delete Alarm** icon. |
| Filter the alarms             | • Enter the information that you want to use as the filter in the **Filters** pane, then click the **Refresh** icon. |
**Add a custom view**

Custom views include components that allow you to display the information you want to see.

**Task**

For option definitions, click ? in the interface.

1. On the views toolbar, click the Create New View icon, then click and drag a component from the View Editing Toolbar (see View components).

2. On the Query Wizard, make selections so that the view generates the data you want displayed (see Working with the Query Wizard), then click Finish.

   The data is displayed in the component that you added.

3. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move the component</td>
<td>Click the component's title bar, then drag and drop it.</td>
</tr>
<tr>
<td>Display host names instead of IP addresses by default</td>
<td>Click the Show host names icon on the toolbar of a component displaying IP addresses (see Managing host names).</td>
</tr>
<tr>
<td>Customize the component</td>
<td>Click the component, then make changes to the settings in the Properties pane (see Customizing components).</td>
</tr>
<tr>
<td>To...</td>
<td>Do this...</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add more components to the view</td>
<td>1 Click and drag a component.</td>
</tr>
<tr>
<td></td>
<td>2 On the Query Wizard, make selections so that the view generates the</td>
</tr>
<tr>
<td></td>
<td>data you want displayed, then click Finish.</td>
</tr>
<tr>
<td>Save the view</td>
<td>1 Click <strong>Save</strong> or <strong>Save As</strong>, then enter a name for the view.</td>
</tr>
<tr>
<td></td>
<td><strong>To save it in an existing folder, select the folder.</strong></td>
</tr>
<tr>
<td></td>
<td>2 Click OK.</td>
</tr>
<tr>
<td>Copy and paste a component</td>
<td>1 Click the component that you want to copy.</td>
</tr>
<tr>
<td></td>
<td>2 Click <strong>Copy</strong>, then click <strong>Paste</strong>.</td>
</tr>
<tr>
<td>Delete a component</td>
<td>Select the component, then click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Exit the view editor without saving a view</td>
<td>Delete all components, then close the <strong>View Editing</strong> toolbar.</td>
</tr>
</tbody>
</table>

### View components

Create custom views to display event, flow, asset, and vulnerabilities data in a way that is most useful to you.

Each view consists of components you select on the View Editing Toolbar and set up to display the data. When you select one, the Query Wizard opens, allowing you to define details about the data displayed in the component.

### Description of view components

There are 13 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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Control Dial" /></td>
<td>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 the ESM console.</td>
</tr>
<tr>
<td></td>
<td>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 <strong>Current Day</strong> and <strong>Total Events</strong> 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 <strong>Average Severity</strong> or <strong>Average Bytes</strong>.</td>
</tr>
<tr>
<td><img src="image" alt="Source and Destination Graph" /></td>
<td>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 (↻).</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Pie Chart</td>
<td>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).</td>
</tr>
<tr>
<td>Table</td>
<td>Displays the query information in several columns. This component is useful to show event and flow data at its finest granularity.</td>
</tr>
<tr>
<td>Bar Chart</td>
<td>Displays the queried information in a bar graph, allowing you to compare the size of each result in a given time range.</td>
</tr>
<tr>
<td>List</td>
<td>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.</td>
</tr>
<tr>
<td>Distribution</td>
<td>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.</td>
</tr>
<tr>
<td>Note Area</td>
<td>A blank component that is used for text-based notes. It allows you to write notes that are related to the current view.</td>
</tr>
<tr>
<td>Count</td>
<td>Displays the total events, assets, vulnerabilities, or flows queried for a specific view.</td>
</tr>
<tr>
<td>Title</td>
<td>Allows you to create a title or heading for your view. It can be placed anywhere on your view.</td>
</tr>
<tr>
<td>Network Topology</td>
<td>Allows you to view the data represented across the network. You can also custom build a view that can be used hand-in-hand with network discovery data (see Add devices to network topology component).</td>
</tr>
<tr>
<td>Geolocation Map</td>
<td>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.</td>
</tr>
<tr>
<td>Filter List</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Customizing components

When you are adding or editing a component, several options are available in the Properties pane that can be used to customize it. The available options depend on the component selected.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Change the title of a component.</td>
</tr>
<tr>
<td>Width and Height</td>
<td>Set the dimensions of the component. You can also click and drag the boundary line.</td>
</tr>
<tr>
<td>X and Y</td>
<td>Set the location of the component on the view. You can also click the title bar of the component, then drag and drop it.</td>
</tr>
<tr>
<td>Edit Query</td>
<td>Make changes to the current query. When you click this button, the Query Wizard opens (see Working with the Query Wizard).</td>
</tr>
<tr>
<td>Show Control Bar</td>
<td>Set whether to display the control bar at the bottom of the component.</td>
</tr>
<tr>
<td>Page Size</td>
<td>Set how many records are displayed per page if there is more data than can be displayed at once.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Show Others Value</td>
<td>If this option is selected, an <strong>Others</strong> value is displayed at the bottom of a chart or list component. It gives the total of all records that are not displayed on the current page. For example, if you are looking at page two of a record set, the <strong>Others</strong> category is the sum of the values from page one and all pages after page two.</td>
</tr>
<tr>
<td>Show Legend</td>
<td>Display a legend below or to the right of a pie chart.</td>
</tr>
<tr>
<td>Show Values</td>
<td>Include the value for each item on a bar chart.</td>
</tr>
<tr>
<td>Show Labels</td>
<td>Include a label for each bar on a bar chart. You can set the maximum number of characters that can be displayed in a label. If it is set at 0, there will be no maximum limit on the label.</td>
</tr>
<tr>
<td>Show baseline averages</td>
<td>Select whether to compare current data with historical data on a distribution or bar chart, or control dial. There are two different options to use when displaying baseline data:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic time range</strong> — If this option is selected, the baseline data is correlated by using the same time period that is being used for the current query for the past five intervals. For example, if you are querying the current day on a Monday, the baseline data is calculated for the same time for the last five Mondays. Fewer intervals are used if no data exists for a given interval. The values that are gathered from each interval are then averaged to calculate the current baseline value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Use specific time range</strong> — Selecting this time range allows you to specify a start and end time that should be used to calculate an average. When this option is used, it is calculated as a single time period. For distribution reports, it produces a flat-line average.</td>
</tr>
<tr>
<td></td>
<td>Baseline data is displayed on distribution charts with a blue line. The line is flat if the <strong>Use specific time range</strong> option was selected or if there is not enough data to calculate a correlated value. The line is curved (assuming different values for each time period are displayed) if a correlated value is calculated. The bar chart displays an arrow indicator at the baseline point for each bar. If the current value is greater than the baseline value, the bar is red above the baseline marker. If the bar chart is displaying rule severity, the bar color does not change for the baseline value.</td>
</tr>
<tr>
<td></td>
<td>An additional option allows you to set a margin value to be displayed with the baseline data. The margin value is calculated from the baseline value. For example, if the baseline value is 100 and the margin above is 20%, the margin value will be calculated as 120. Turning this feature on displays the margin area for each bar in a bar chart. A distribution chart calculates the average value of the baseline and displays a shaded area above and below the baseline that indicates the margin area.</td>
</tr>
<tr>
<td>Device List</td>
<td>Drag and drop devices to the <strong>Network Topology</strong> component or the <strong>Logical Device Groupings</strong> tree.</td>
</tr>
<tr>
<td>Logical Device Groupings</td>
<td>Create folders to group the devices for the <strong>Network Topology</strong> component.</td>
</tr>
<tr>
<td>Background</td>
<td>Select the color of the background of the view. <strong>Background Image URL</strong> allows you to import an image to use as the background.</td>
</tr>
</tbody>
</table>

**Add devices to network topology component**

Network topology allows you to get event and flow data from the devices or device tree and view the data represented across the network.

**Before you begin**

You must discover your network before the list of devices appears (see **Network discovery**).
It also allows you to custom build a view that can be used with network discovery data. Once you have created a network topology view, you must customize it to display the event or flow information (see Add a custom view).

**Task**

For option definitions, click ? in the interface.

1. When you are adding or editing a view, click, drag, and drop the Event Network Topology component.

   The Properties pane displays the Device List and the Logical Device Groupings tree.

2. From the Device List or Folder List, select a device or folder and do one of the following:
   - To add the device or folder to the component, drag and drop it on the component.
   - To add the device or folder to a group in the Logical Device Groupings tree, click Add, enter a name for the folder and click OK, then drag and drop the device in the folder.

3. Arrange the devices.

   Devices that are physically connected to the system connect with a straight black line on the component. Blue or red curved lines indicate a data path.

**Device details on Network Topology components**

You can view specific device details on a Network Topology component when you double click a device. This screen allows you to view interface and endpoint information such as port summary, total devices, and status of devices.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Summary for</td>
<td>Shows which port you are currently viewing.</td>
</tr>
<tr>
<td>Total</td>
<td>Gives the total number of devices.</td>
</tr>
<tr>
<td>Above Baseline Average</td>
<td>States the number of devices above the current baseline average</td>
</tr>
<tr>
<td></td>
<td>Represents a work station.</td>
</tr>
<tr>
<td></td>
<td>Indicates that the interface has alert data associated with it, and the data is below the baseline average.</td>
</tr>
<tr>
<td></td>
<td>Indicates that the interface has alert data associated with it, and the data is above the baseline average.</td>
</tr>
<tr>
<td></td>
<td>Indicates that the interface has no alert data associated with it.</td>
</tr>
<tr>
<td></td>
<td>Indicates that the administrative state is down (not just operationally down).</td>
</tr>
<tr>
<td></td>
<td>Represents a router.</td>
</tr>
<tr>
<td></td>
<td>Indicates that the switch port is up.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>--------</td>
<td>------------</td>
</tr>
<tr>
<td>![Question Mark]</td>
<td>Represents an unknown device.</td>
</tr>
<tr>
<td>![Map]</td>
<td>Represents an unmanaged device.</td>
</tr>
<tr>
<td>![Error]</td>
<td>Indicates that the ESM can’t communicate with the device through SNMP, network discovery, or ping.</td>
</tr>
</tbody>
</table>

### Component toolbar

The component toolbar, located at the bottom of each component in a view, provides several actions you can perform to the data on the component. The available actions depend on the type of component.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Checkmark]</td>
<td>Mark event(s) as reviewed — Mark specific events once you have reviewed them. You can then use the Change event state filter drop-down list to show only reviewed events or only events that haven’t been reviewed.</td>
</tr>
</tbody>
</table>
| ![File] | Assign events to a case or remedy — Assign events to a case (see Manage Cases) or send an email message to the Remedy system (if one is set up). When you click this icon, you can select: 
  - Create a new case 
  - Add events to a case 
  - Send event to Remedy (see Send a Remedy Email) |
| ![Globe] | Launch device URL — Launch the URL that is associated with the selected event, if you added one for the device (see Add a URL). If you did not define one, you are prompted to add it. |
| ![Trash Can] | Show or Hide host names — Show or hide the host names associated with the IP addresses on the view (see Managing host names). |

**Chart type icons**

<p>| Definition | Change chart type — Change the type of chart displaying the data. The icon for this feature will be the component icon for the current chart type. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>View or Hide data details — Show or hide details about the selected event. There are several tabs in this section:</td>
<td></td>
</tr>
<tr>
<td>Details:</td>
<td>Shows the available information for the event or flow selected.</td>
</tr>
<tr>
<td>Advanced Details:</td>
<td>Shows information regarding the source network device, destination network device, and remedies. You can search for events or flows by their IDs, if you have sufficient rights to view those records, by clicking the magnifying glass icon to the right of the Event ID or Flow ID field.</td>
</tr>
<tr>
<td>Geolocation:</td>
<td>Shows the location of the source and destination of the selected event.</td>
</tr>
<tr>
<td>Description:</td>
<td>Gives the name, description and signature or rule associated with the event.</td>
</tr>
<tr>
<td>Notes:</td>
<td>Allows you to add notes to the event or flow, which appear each time you view that particular item.</td>
</tr>
<tr>
<td>Packet:</td>
<td>Retrieves the contents of the packet that generated the selected event. You can perform the following functions on this tab:</td>
</tr>
<tr>
<td>Select the format to view the packet.</td>
<td></td>
</tr>
<tr>
<td>Retrieve the packet data by clicking <img src="image" alt="button" />.</td>
<td></td>
</tr>
<tr>
<td>Save the packet on your computer by clicking <img src="image" alt="button" />. If it is a packet capture (PCAP) (such as Nitro IPS events, ADM events, Estreamer events from the Receiver), it will be saved with a .pcap extension and can be opened in any PCAP-viewing program. If it isn’t, it will be saved as a text file.</td>
<td></td>
</tr>
<tr>
<td>Set it to retrieve the packet automatically when you click an event.</td>
<td></td>
</tr>
<tr>
<td>Search for information in the packet by entering the keyword in the Find text field and clicking <img src="image" alt="button" />. Do not use special characters such as brackets or parentheses in the Find text field.</td>
<td></td>
</tr>
<tr>
<td>Source Events:</td>
<td>When a correlation or vulnerability event is selected, displays the set of events that caused the event to be generated.</td>
</tr>
<tr>
<td>ELM Archive:</td>
<td>If you enter text in the Find Text field, retrieves data that is archived on the ELM. If the event is aggregated, a Receiver or ACE device will display up to 100 aggregated events.</td>
</tr>
<tr>
<td>Custom Types:</td>
<td>If you defined custom types (see Custom type filters), shows the custom type fields and the data from this event that belongs in these fields.</td>
</tr>
<tr>
<td>Information:</td>
<td>Shows information such as device name, IP address, operating system and device version, system</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>• Interfaces</td>
<td>Shows the port name, port speed, VLAN, administrative state, and operational state.</td>
</tr>
<tr>
<td>• Neighbors</td>
<td>Shows specific information regarding the neighboring devices such as local interface, neighbor device, and neighbor interface.</td>
</tr>
<tr>
<td>Change interval period and rate</td>
<td>Set how often you want the data in the chart to be refreshed.</td>
</tr>
<tr>
<td>Set rate</td>
<td>Select the rate for the data that is displayed (none, per second, per minute, per hour, per day, per week, per month).</td>
</tr>
<tr>
<td>IP address</td>
<td>View the source and destination events or flows for a specific IP address. Type the address in the field or select one that you have used previously and click the Refresh icon.</td>
</tr>
<tr>
<td>Geolocation options</td>
<td>Switch between marking city, state, country, and world areas; zoom in and out; and select locations using the Ctrl and Shift keys.</td>
</tr>
<tr>
<td>Change page</td>
<td>Navigate through the data when there is more than one page.</td>
</tr>
<tr>
<td>Change event state filter</td>
<td>Select the type of events or flows to display in the analysis list. You can view all events, only events that have been reviewed, only events that have not been reviewed, events that have been remedied, all flows, open flows only, or closed flows only.</td>
</tr>
<tr>
<td>History Buttons</td>
<td>Scroll forward and backward through the changes made on the view.</td>
</tr>
<tr>
<td>View Data Paths or Hide Data Paths</td>
<td>Hide or view the line that connects two devices with event or flow data connections.</td>
</tr>
<tr>
<td>Hide Text</td>
<td>Hide or show the labels on the device in the Network Topology view.</td>
</tr>
</tbody>
</table>

**Send a remedy email**

If you set up a remedy system, you can send an email message to notify the system of an event that requires a remedy. When you follow this process, you receive a remedy case number to add to the event record.

A remedy system is set up by the user and has no connection to McAfee Nitro IPS.

**Task**

For option definitions, click ? in the interface.

1. On an event view, highlight the event that requires remedial action.
2. Click the **Assign events to a case or Remedy** icon, then select **Send event to Remedy**.
3. Add the **Prefix**, **Keyword**, and **Enterprise User ID**.
4. (Optional) Add information under **Details**, which contains information generated by the system regarding the event.

5. Click **Send**.

**Component menu options**

Most components on a view have a menu that lists the component’s available options. This table lists the possible items.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Drilldown (Event, Flow, Asset)</strong></td>
<td>View further details for the data type you select on the drill-down lists. A new view displays the details.</td>
</tr>
<tr>
<td><strong>Summarize or Summarize by</strong></td>
<td>View other event or flow data that shares characteristics of the events you selected. For example, if you are looking at a port scan event on the analysis screen and you want to see other events generated by the same attacker, click the event, select <strong>Summarize By</strong>, then click <strong>Source IP</strong>.</td>
</tr>
<tr>
<td><strong>Modify aggregation settings</strong></td>
<td>Create an exception to the general aggregation settings for an individual rule (see <em>Add exceptions to event aggregation settings</em>).</td>
</tr>
<tr>
<td><strong>Create new watchlist</strong></td>
<td>Select events on a view and add them to a new watchlist (see <em>Watchlists</em>).</td>
</tr>
<tr>
<td><strong>Append to watchlist</strong></td>
<td>Select events on a view and add them to an existing watchlist.</td>
</tr>
<tr>
<td><strong>Create new alarm</strong></td>
<td>Select events on a view and create an alarm based on their values (see <em>Create an alarm</em>).</td>
</tr>
<tr>
<td><strong>Perform MVM scan</strong></td>
<td>Initiate a McAfee Vulnerability Manager scan if your system includes is an McAfee Vulnerability Manager device.</td>
</tr>
<tr>
<td><strong>Launch ePO</strong></td>
<td>Open the ePolicy Orchestrator interface (see <em>Launch ePolicy Orchestrator</em>).</td>
</tr>
<tr>
<td><strong>TIE Execution History</strong></td>
<td>When a TIE event is selected, open the TIE Execution History page to view the IP addresses that have attempted to execute the selected file. From this page you can create a new watchlist, append a file to a watchlist, create a new alarm, blacklist a file, export a file to CSV, or add ePolicy Orchestrator tags to the file.</td>
</tr>
<tr>
<td><strong>Show Rule</strong></td>
<td>View the rule that generated the event.</td>
</tr>
<tr>
<td><strong>IP Address details</strong></td>
<td>Look up information about a source or destination IP address or port. You can view threat details and the results of the WHOIS Lookup for the selected IP address.</td>
</tr>
<tr>
<td><strong>ASN Lookup</strong></td>
<td>Retrieve a WHOIS record using the ASN identifier.</td>
</tr>
<tr>
<td><strong>Browse Reference</strong></td>
<td>Open your default web browser and connect to the McAfee online signature database, which provides information about the signature that generated the selected event.</td>
</tr>
<tr>
<td><strong>Set Remedy Case ID</strong></td>
<td>Add the remedy case ID, which you received when you sent an event email to the Remedy system, to the event record for future reference (see <em>Add remedy case ID to event record</em>).</td>
</tr>
<tr>
<td><strong>Blacklist</strong></td>
<td>Add the IP address from the selected event to the blacklist. Selecting this option opens the <strong>Blacklist Editor</strong>, which has the IP address field populated with the data from the selected event (see <em>IPS or virtual device blacklist</em>).</td>
</tr>
<tr>
<td><strong>Search ELM</strong></td>
<td>Perform a search for information contained on the ELM about the event that you select. The <strong>Enhanced ELM Search</strong> page opens, populated with the data you select (see <em>Perform an enhanced ELM search</em>).</td>
</tr>
<tr>
<td><strong>Change VLAN</strong></td>
<td>Change the VLAN for any selected device. You can select from 1–12 devices.</td>
</tr>
<tr>
<td>Option</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Disable or Enable Port(s)</td>
<td>Single or multi-select any interface or endpoint. Depending on what you select, the disable or enable option appears. For example, if you select five interfaces and one is enabled and the other four are disabled, you can only disable the port. However, if you select one port that is disabled, the Enable Port(s) option is available.</td>
</tr>
<tr>
<td>View Events or View Flows</td>
<td>View the events generated by a flow or the flows generated by an event.</td>
</tr>
<tr>
<td>Export</td>
<td>Export a view component to PDF, text, CSV, or HTML format (see Export a component).</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete events or flows from the database. You must belong to a group with event privileges and you can delete only the records that are currently selected, the current page of data, or a maximum number of pages starting at page 1.</td>
</tr>
<tr>
<td>Mark as reviewed</td>
<td>Flag events as reviewed. You can mark all the records in the result set, the current page, or selected records.</td>
</tr>
<tr>
<td>Create custom firewall rule</td>
<td>Create a custom firewall rule based on properties of the selected event or flow. When you click Create Custom Firewall Rule, the New Rule page opens (see Add custom ADM, database, or correlation rule).</td>
</tr>
<tr>
<td>Create custom rule</td>
<td>Create a custom rule using the signature that triggered a particular alert as a starting point. This option is available when you select alerts generated by standard (non-firewall) rules. When you click Create Custom Rule, the New Rule page opens (see Add custom ADM, database, or correlation rule).</td>
</tr>
</tbody>
</table>

**Perform a WHOIS or ASN lookup**

On a table component, you can perform a WHOIS lookup to find information about a source or destination IP address. ASN Lookup, available on any ASN query on a bar chart and any flow record on a table component that has ASN data, retrieves a WHOIS record using the ASN identifier.

**Task**

For option definitions, click ? in the interface.

1. Select an IP address or flow record with ASN data listed on a table component, or an ASN query bar on a bar chart component.

2. Click the menu, then select IP Address Details or ASN Lookup.

3. To look up another IP address or identifier:
   - On the WHOIS tab page, select an IP address from the drop-down list and enter the host name.
   - On the ASN Lookup page, type in the numbers or select one from the drop-down list.

**Add remedy case ID to event record**

When you send an event email to the remedy system, you receive a Case ID number. You can add it to the event record for reference purposes.

**Task**

For option definitions, click ? in the interface.

1. Highlight the event on the Event Analysis view, then click the menu.

2. Select Set Remedy Case ID, type the number, and click OK.
Export a component
You can export the data on an ESM view component. Chart components can be exported in text or PDF formats and table components in common separated values (CSV) or HTML.

When exporting the current page of a chart, distribution, or table component on a view, the exported data matches exactly what you see when you initiate the export. If you export more than one page, the query runs again as it exports the data, so it might be different from what you see on the component.

Task
For option definitions, click ? in the interface.

1 On a view, click the menu for the component you want to export, then click Export.

2 Select one of the following formats:
   - Text — Export the data in text format.
   - PDF — Export the data and an image.
   - Image to PDF — Export only the image.
   - CSV — Export a list in comma-delimited format.
   - HTML — Export the data in a table.

3 On the Export page, specify the data that you want to export.
   - If you selected Text or PDF, you can export the current page of data or a maximum number of pages starting at page 1.
   - If you selected Image to PDF, the image is generated.
   - If you selected CSV or HTML, you can export only the selected items, just the current page of data, or a maximum number of pages, starting at page 1.

4 Click OK
The export file is generated and you are prompted to download the resulting file.

Working with the Query Wizard
Each report or view on the ESM gathers data based on the query settings for each component.

When adding or editing a view or report, define the query settings for each component on the Query Wizard by selecting the query type, the query, the fields to include, and the filters to use. All the queries on the system, both predefined and custom, are listed on the wizard so you can select the data you want gathered by the component. You can also edit or remove queries, and copy an existing query to use as a template to set up a new query.

Manage queries
The ESM comes with predefined queries that you can select on the Query Wizard when adding or editing a report or view. You can edit some of the settings on these queries and you can add and remove custom queries.

Task
For option definitions, click ? in the interface.

1 Do one of the following to access the Query Wizard.
<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| **Add a new view** | 1 Click the **Create New View** icon located on the view toolbar.  
2 Drag-and-drop a component from the **View Editing Toolbar** to the view pane.  
The **Query Wizard** opens. |
| **Edit an existing view** | 1 Select the view you want to edit.  
2 Click the **Edit Current View** icon located on the view toolbar.  
3 Click the component that you want to edit.  
4 Click **Edit Query** in the **Properties** pane.  
The **Query Wizard** opens on the second page. |
| **Design the layout for a new report** | 1 On **System Properties**, click **Reports**.  
2 Click **Add**.  
3 In section 5 of the **Add Report** page, click **Add**.  
4 Drag and drop a component in the report layout section.  
The **Query Wizard** opens. |
| **Edit the layout on an existing report** | 1 On **System Properties**, click **Reports**.  
2 Select the report to edit, then click **Edit**.  
3 In section 5 of the **Edit Report** page, select an existing layout, then click **Edit**.  
4 Click the component in the report layout section, then click **Edit Query** in the **Properties** section.  
The **Query Wizard** opens on the second page. |

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

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| **Add a new query** | 1 Select the query that you want to use as a template, then click **Copy**.  
2 Type the name for the new query, then click **OK**.  
3 On the list of queries, click the one that you just added, then click **Next**.  
4 On the second page of the wizard, change the settings by clicking the buttons. |
| **Edit a custom query** | 1 Select the custom query that you want to edit, then click **Edit**.  
2 On the second page of the wizard, change the settings by clicking the buttons. |
| **Remove a custom query** | Select the custom query that you want to remove, then click **Remove**. |

3 Click **Finish**.
**Bind components**
When a view component is linked to another component using data binding, the view becomes interactive.

Selecting one or more items in the parent component causes the results displayed in the child component to change, as if a drill-down was executed. For example, if you bound a parent bar chart source IP component to a child bar chart destination IP component, making a selection in the parent component causes the child component to execute its query using the selected source IP as a filter. Changing the selection in the parent component refreshes the data in the child component.

*Task*
For option definitions, click ? in the interface.

1. Create the parent and child components, then select the child component.
2. On the Properties pane, click Edit Query | Filters.
   
   The Query Filters page opens with the parent and child queries enabled.
3. From the child query drop-down list, select Bind to.
4. Click OK, then click Finish.

**Comparing values**
Distribution graphs have an option that allows you to overlay an additional variable on top of the current graph.

In this way, two values can be compared to easily show the relationships, for example, between total events and average severity. This feature provides valuable data comparisons over time, at a glance. This feature is also useful for saving screen real-estate when building large views, by combining results onto a single distribution graph.

The comparison is limited to the same type as the selected query. For example, if an event query is selected, you can compare with the fields from the event table only, not the flow or assets and vulnerabilities table.

When you apply the query parameters to the distribution chart, it runs its query as normal. If the comparison field is enabled, a secondary query is run for the data at the same time. The distribution component displays the data for both data sets on the same graph, but uses two separate vertical axes. If you change the chart type (lower-right corner of component), both sets of data continue to display.

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

*Task*
For option definitions, click ? in the interface.

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 for views and reports
Set up the distribution component on a view or report so that you can see the distribution of events related to a specific field.

You can select the field to stack by when you add the component to a view or report. When you access the view, you can change the settings, set the time interval, and set the chart type and details.

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

#### Task
For option definitions, click ? in the interface.

1 Drag and drop the **Distribution** component on a view (see **Add a custom view**) or a report (see **Add report layout**), then select the type of query.

> Stacking is not available for **Collection Rate** or **Average** (for example, **Avg Severity Per Alert** or **Avg Duration Per Flow**) distribution queries.

2 On the second page of the **Query Wizard**, click **Stacking**, then select the options.

3 Click **OK** on the **Stacking Options** page and **Finish** on the **Query Wizard**.

The view is added. You can change the settings, and set the time interval and chart type by clicking the **Chart Options** icon.

### Manage views
Managing views provides a quick way for you to copy, import, or export more than one view at a time, as well as select the views to include on the list of views and assign permission for specific users or groups to access individual views.

#### Task
For option definitions, click ? in the interface.

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

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

### Look around an event
From the **Event Analysis** view, you can look for events that match one or more of the fields in the event within the time frame you select before and after the event.
**Task**
For option definitions, click ? in the interface.

1. On the ESM console, click the views list, then select Event Views | Event Analysis.
2. Click an event, click the menu icon, then click Look Around.
3. Select the number of minutes before and after the time of the event that you want the system to search for a match.
4. Click Select filter, select the field that you want the search to match on, then type the value.

The results are displayed on the Look Around Results view.

*If you leave this view, then want to return to it later, click Last Look Around on the Event Analysis menu.*

**View the IP address details of an event**
If you have a McAfee® Global Threat Intelligence™ (McAfee GTI) license from McAfee, you have access to the new Threat Details tab when you perform an IP Address Details lookup. When you select this option, details about the IP address are returned, including risk severity and geolocation data.

**Before you begin**
Purchase a McAfee GTI license (see McAfee GTIWatchlist).

*If your McAfee GTI license has expired, contact your McAfee Sales Engineer or McAfee support.*

**Task**
For option definitions, click ? in the interface.

1. On the ESM console, select a view that includes a table component such as Event Views | Event Analysis.
2. Click an IP address, click the menu icon on any component that has an IP address, then click IP Address Details.

The Threat Details tab lists the data for the selected IP address. You can copy the data to the system clipboard.

*The IP Address Details option has replaced the WHOIS Lookup option on the context menu. However, the IP Address Details page includes a WHOIS Lookup tab that shows this information.*

**Change the default view**
The Default Summary view appears in the view pane by default when you first log on to the ESM console. You can change this default view to any of the predefined or custom views on the ESM.

**Task**
For option definitions, click ? in the interface.

1. On the ESM console navigation bar, click Options, then select Views.
2. On the Default System View drop-down list, select the new default view, then click OK.
Filtering views

In the filters pane located on the main ESM console, you can set up filters to be applied to views. Any filters that are applied to a view are carried forward to the next view that is opened.

When you first log on to the ESM, the default filters pane includes the Source User, Destination User, Source IP, and Destination IP filter fields. You can add and delete filter fields, save filter sets, change the default set, manage all filters, and launch the string normalization manager.

An orange funnel icon appears in the upper-right corner of the view pane to alert you when filters are applied to the view. If you click this orange icon, all filters are cleared and the query is executed again.

Anywhere you have comma-separated filter values such as variables, global filters, local filters, normalized strings, or report filters, you must use quotes if they are not part of a watchlist. If the value is Smith,John, you must type "Smith,John". If there are quotes in the value, you must enclose the quotes in quotes. If the value is Smith,"Boy"John, you must enter it as "Smith,\"Boy\"John".

You can use contains and regex filters (see Description of contains and regex filters).

Filter a view

Filters help you view details about selected items on a view. If you enter filters and refresh the view, the data in the view reflects the filters you added.

Task

For option definitions, click ? in the interface.

1. On the ESM console, click the drop-down list of views, then select the view you want to filter.

2. In the Filter pane, fill in the fields with the data you want to filter on in one of these ways:
   - Type the filter information in the appropriate field. For example, to filter the current view to see only the data that has a source IP address of 161.122.15.13, type the IP address in the Source IP field.
   - Type a contains or regex filter (see Description of contains and regex filters).
   - Click the Display filter list icon next to the field and select the variables or watchlists to filter on.
   - On the view, select the data you want to use as the filter, then click the field on the Filter pane. If the field is blank, it is auto-populated with the data you selected.

   For Average Severity, use a colon (:) to enter a range. For example, 60:80 is a severity range of 60 to 80.

3. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View data that matches more than one filter</td>
<td>Enter the values in each field.</td>
</tr>
<tr>
<td>View data that matches some filter values and excludes others</td>
<td>Enter the filter values that you want to include and exclude.</td>
</tr>
<tr>
<td></td>
<td>2 Click the NOT icon next to the fields you want to exclude.</td>
</tr>
</tbody>
</table>
To... Do this...

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 marked OR, and matches either of the values in the fields marked OR.

At least two fields must be marked OR for this filter to work.

Make the filter values case-insensitive Click the Case-insensitive icon next to the appropriate filter field.

Replace normalized strings with their aliases Click the string normalization icon next to the appropriate filter field.

4 Click the Run Query icon.

The view is refreshed and the records matching the values you entered are displayed in the view. An orange filter icon appears in the upper-right corner of the view pane, indicating that the data in the view is a result of filters. If you click the icon, the filters are cleared and the view shows all the data.

Filters pane
The filters pane provides options to help you set filters for the views.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Hints" /></td>
<td>Hints</td>
<td>Have a tooltip appear when you click in a filter field.</td>
</tr>
<tr>
<td><img src="image" alt="Launch string normalization manager" /></td>
<td>Launch string normalization manager</td>
<td>Filter on a string and its aliases (see String normalization).</td>
</tr>
<tr>
<td><img src="image" alt="Run query" /></td>
<td>Run query</td>
<td>Apply the current filters to the view. You must click this icon when you change a filter value and want to apply it to the current view.</td>
</tr>
<tr>
<td><img src="image" alt="Clear all" /></td>
<td>Clear all</td>
<td>Clear all filters from the filters pane.</td>
</tr>
</tbody>
</table>
| ![Filter set options](image) | Filter set options | Select an action to take with the filter sets.  
• Make Default — Saves the filter values that you entered as your default. These filters are applied automatically when you log on.  
• Restore Default — Reverts the filters to your default values so that you can run the query on the default filter set.  
• Save Populated Filters — Saves the current filter set and adds it to the list of available filters, where you select it when adding a filter. Type a name for the set, then select the folder where you want to save the set.  
• Manage Filters — Opens the Managing Filter Sets page, where you organize the available filter sets. |
| ![Enter a Field or Filter Set](image) | Enter a Field or Filter Set | Select a filter field or filter set to filter the view by. When you click the field, a drop-down menu lists all possible filters and filter sets. |
| ![Display filter list](image) | Display filter list | Select the variables or watchlists to filter on. |
| ![NOT](image) | NOT | To view data that matches some filter values and excludes others, click next to the fields that you want to exclude. |
Add UCF and Windows event ID filters

One of the challenges for regulation compliance support is the ever-changing nature of regulations. Unified Compliance Framework (UCF) is an organization that maps the specifics of each regulation to harmonized control IDs. As regulations change, these IDs are updated and pushed to the ESM.

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

<table>
<thead>
<tr>
<th>To do...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| 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.

Watchlists

A watchlist is a grouping of a specific type of information that can be used as a filter or as an alarm condition.

It can be global or specific to a user or group and can be static or dynamic. A static watchlist consists of specific values that you enter or import. A dynamic watchlist consists of values that result from a regular expression or string search criteria that you define.

A watchlist can include a maximum of 1,000,000 values. The list of values on the Add Watchlist or Edit Watchlist pages can display up to 25,000 values. If there are more, you are informed that there are too many values to display. If you want to edit a watchlist by adding values that increase the total number to more than 25,000, you must export the existing list to a local file, add the new values, then import the new list.
You can set up the values on a watchlist to expire. Each value is time-stamped and expires when the duration specified is reached, unless it refreshes. Values refresh if an alarm triggers and adds them to the watchlist. You can refresh the values set to expire by appending them to the list using the `Append to watchlist` option on the menu of a view component (see Component menu options).

The ESM provides a connector to the relational data source in Hadoop HBase, using the key-value pairs from the source. This data can be used in a watchlist (see Add Hadoop HBase watchlist). For example, it can be fed into alarms that trigger when values in the watchlist are found in new events.

**Add a watchlist**
Add a watchlist to the ESM so that you can use it as a filter or in an alarm condition.

**Task**
For option definitions, click ? in the interface.

1. Access the **Watchlists** page in one of these ways:
   - On the ESM console, click the **Watchlists** quick launch icon.
   - On the system navigation tree, click **System Properties**, then click **Watchlists**.

   The **Watchlists** table shows all watchlists on the system.

   **GTI Malicious IPs** and **GTI Suspicious IPs** appear on the table, but don’t contain data unless you purchased a McAfee GTI license from McAfee. Contact your McAfee Sales Engineer or McAfee support to purchase a license.

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

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

**See also**
*McAfee GTI watchlist* on page 258

**McAfee GTI watchlist**
McAfee GTI watchlists contain more than 130 million suspicious and malicious IP addresses and their severities, gathered by McAfee. These watchlists can be used to trigger alarms, to filter data in reports and views, as a filter in rule correlation, and as a scoring source for a Risk Correlation Manager on an ACE.

To add the data from the lists to your system, you must purchase a McAfee GTI license from McAfee. Once you do, the lists are added to your system the next time you download rules. This process can take several hours due to the size of the database.

You must have an Internet connection to download the lists. They can’t be downloaded off line.

These lists cannot be viewed or edited, but the **Watchlists** table (**System Properties | Watchlists**) indicates whether the list is **active** (contains values) or **inactive** (does not contain values).

To purchase the McAfee GTI license, contact your McAfee Sales Engineer or McAfee Support.

**Create a watchlist of threat or IOC feeds from the Internet**
You can create a watchlist that can be refreshed periodically to automatically pull threat or Indicator of Compromise (IOC) feeds from the Internet.

On this watchlist, you can preview the data to be retrieved through the HTTP request, as well as add regular expressions to filter this data.
**Task**

For option definitions, click ? in the interface.

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

The **Raw data** field on the **Parsing** tab is populated with the first 200 lines of the html source code. It is just a preview of the web site, but is enough for you to write a regular expression to match on. A **Run Now** or scheduled update of the watchlist includes all matches from your regular expression search. This feature supports RE2 syntax regular expressions, such as \(\text{\(d\{1,3\}\.d\{1,3\}\.d\{1,3\}\.d\{1,3\}\)}\) to match on an IP address.

**Add a Hadoop HBase watchlist**

Add a watchlist using Hadoop HBase as the source.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, click the **Properties** icon, then click **Watchlists**.
2. On the **Main** tab of the **Add Watchlist** wizard, select **Dynamic**, enter the information requested, then click the **Source** tab.
3. Select **Hadoop HBase (REST)** in the **Types** field, then type the host name, port, and name of the table.
4. On the **Query** tab, fill in the lookup column and query information:
   a. Format Lookup Column as **columnFamily:** **column**
   b. Populate the query with a scanner filter, where the values are Base64 encoded. For example:

```xml
<Scanner batch="1024"> 
<filter> 
  | 
  "type": "SingleColumnValueFilter",
  "op": "EQUAL",
  "family": "ZW1wbG95ZWVJbmZv",
  "qualifier": "dXNlcm5hbWU=",
  "latestVersion": true,
  "comparator": {
  "type": "BinaryComparator",
  "value": "c2NhcGVnb2F0"
  }
</filter>
</Scanner>
```
5. Click the **Values** tab, select the value type, then click the **Run Now** button.
String normalization

Use string normalization to set up a string value that can be associated with alias values and to import or export a .csv file of string normalization values.

This enables you to filter the string and its aliases by selecting the string normalization icon next to the appropriate field in the Filter pane. In the case of the John Doe user name string, you define a string normalization file where the primary string is John Doe and its aliases are, for example, DoeJohn, JDoe, john.doe@gmail.com, and JohnD. You can then enter John Doe in the User_Nickname filter field, select the string normalization filter icon next to the field, and refresh the query. The resulting view displays all events associated with John Doe and his aliases, enabling you to check for login inconsistencies where source IPs match but user names do not. This feature can also assist you in meeting regulations requiring that you report privileged user activity.

Manage string normalization files

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

**Task**

For option definitions, click ? in the interface.

1. On the Filters pane, click the Launch string normalization manager icon.
2. Perform any of the available actions, then click Close.

Create a string normalization file to import

If you create a .csv file of aliases, you can import it on the String Normalization page so that it can be used as a filter.

**Task**

For option definitions, click ? in the interface.

1. In a text or spreadsheet program, type the aliases using this format:
   
   \[
   \text{command, primary string, alias}
   \]

   Possible commands are add, modify, and delete.
2. Save it as a .CSV file, then import the file.

Custom type filters

Custom type fields can be used as filters for views and reports and to create custom rules, to define and then access data that is most relevant to you.

The data generated by these custom type fields can be viewed in the Details section of the Event Analysis or Flow Analysis view.

You can add, edit, or remove custom types as well as export and import them. Use the Edit page to change the name. If it is a custom data type, you can also change the subtype settings.

**Export or import custom types**

When you export custom types, all are exported to the location that you select. When you import a file of custom types, the imported data replaces the current custom types on the system.
Custom queries
When you are setting up a custom query for a view, the predefined custom types appear as options when you are selecting the fields for the query. If you add a custom type as a field in the query, it acts as a filter. If the information that you are querying has no data for that custom type, the query table returns with no results. To avoid this, select the user field (Custom Field 1 through 10 in the Event Field column of the table) that returns the results that you need instead of using the custom type.

For example, let's say you want the query results to include source user data, if there is any. If you select Source User as a query field, it acts as a filter and, if the information you are querying has no source user data, the query returns no results. However, if you select User Field 7, which is designated as the user field for source user, it doesn't act as a filter and appears as a column in the table of results. If there is source user data, it appears in this column. If there isn't data for this field, the User Field 7 column is blank but other columns are populated.

Custom data type
When you select Custom in the Data Type field, you can define the meaning of each field in a multiple field log.

For example, a log (100300.351) contains three fields (100, 300.35, 1). The custom subtype allows you to specify what each of these fields is (integer, decimal, Boolean). For example:
• Initial log — 100300.351
• 3 Subtypes — Integer|decimal|boolean
• Custom Subtype — 100|300.35|1

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

Name/value custom type
If you select the Name/Value Group data type, you can add a custom type that includes a group of name/value pairs that you specify. You can then filter views and queries by these pairs, and use them in field match alarms.

These are some of the characteristics of this feature:
• The name/value group fields must be filtered using a regular expression.
• The pairs can be correlated so they are selectable in the Correlation rule editor.
• The values part of the pair can only be collected through the Advanced Syslog Pareser (ASP).
• The maximum size for this custom type is 512 characters, which include the names. If it is larger than that, the values are cut off when collected. McAfee recommends that you limit the size and number of names.
• The names must consist of more than two characters.
• The name/value custom type can have up to 50 names.
• Each name in the name/value group is displayed in the global filter as <name of the group> - <name>.

Regular expression format for non-indexed custom types
Follow this formatting for non-indexed and indexed string, random string, and hashed string custom types:
You can use `contains(<regular expression>)` syntax or just type a value into the non-indexed random string or hashed string fields, then filter custom types.

You can use `regex()` syntax.

With `contains()`, if you put a comma-separated filter into a non-indexed custom type field (Tom,John,Steve), the system performs a regular expression. The comma and asterisk act as a bar (|) and a period followed by the asterisk (.* in a `contains` or non-indexed random string or hashed string field. If you type a character such as an asterisk (*), it is replaced with a period followed by the asterisk (.*).

An invalid regular expression or a missing closing or opening parenthesis can cause an error telling you that you have a bad regular expression.

You can only use a single `regex()` or `contains()` in non-indexed and indexed string, random string, and hashed string custom type filter fields.

The Signature ID field now accepts `contains(<on part or all of a rule message>)` and `regex(<on part of a rule message>)`.

A common search filter for `contains` is a single value, not a single value with a .* before and after. Here are some common search filters:

- A single value
- Multiple values separated by commas, which are converted into a regular expression
- A `contains` statement with a * that acts like .*
- Advanced regular expressions, where you can use the `regex()` syntax

See Description of `contains` and `regex` filters.

Create custom types

Add custom types to use as filters if you have administrator privileges.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, select **System Properties**, then click **Custom Types**.
2. Click **Add**, then complete the requested information.
3. Click **OK** to save the custom type.

Predefined custom types table

If you have administrator privileges, you can view a list of the predefined custom types on the custom types table (**System Properties** | **Custom Types**). If you do not have administrator privileges, use this list of predefined custom types.

<table>
<thead>
<tr>
<th>Name</th>
<th>Data type</th>
<th>Event field</th>
<th>Flow field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>String</td>
<td>Custom Field - 1</td>
<td>None</td>
</tr>
<tr>
<td>Application_Layer</td>
<td>Signature ID</td>
<td>None</td>
<td>Custom Field - 4</td>
</tr>
<tr>
<td>Application_Protocol</td>
<td>String</td>
<td>Custom Field - 1</td>
<td>None</td>
</tr>
<tr>
<td>Authoritative_Answer</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>Bcc</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Name</td>
<td>Data type</td>
<td>Event field</td>
<td>Flow field</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------</td>
<td>------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Cc</td>
<td>String</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>Client_Version</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Command</td>
<td>String</td>
<td>Custom Field - 2</td>
<td>None</td>
</tr>
<tr>
<td>Confidence</td>
<td>Unsigned Integer</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>Contact_Name</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>Cookie</td>
<td>String</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>Database_Name</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Destination User</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>Custom Field - 1</td>
</tr>
<tr>
<td>Destination_Filename</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Direction</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>DNS_Class</td>
<td>String</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>DNS_Name</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>DNS_Type</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>Domain</td>
<td>String</td>
<td>Custom Field - 3</td>
<td>None</td>
</tr>
<tr>
<td>End_Page</td>
<td>Unsigned Integer</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>File_Operation</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>File_Operation_Succeeded</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>Filename</td>
<td>String</td>
<td>Custom Field - 3</td>
<td>None</td>
</tr>
<tr>
<td>Flow_Flags</td>
<td>Unsigned Integer</td>
<td>None</td>
<td>Custom Field - 1</td>
</tr>
<tr>
<td>From</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>Hops</td>
<td>Unsigned Integer</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>Host</td>
<td>String</td>
<td>Custom Field - 4</td>
<td>None</td>
</tr>
<tr>
<td>HTTP_Layer</td>
<td>Signature ID</td>
<td>None</td>
<td>Custom Field - 5</td>
</tr>
<tr>
<td>HTTP_Req_Cookie</td>
<td>String</td>
<td>None</td>
<td>Custom Field - 3</td>
</tr>
<tr>
<td>HTTP_Req_Host</td>
<td>String</td>
<td>None</td>
<td>Custom Field - 5</td>
</tr>
<tr>
<td>HTTP_Req_Method</td>
<td>String</td>
<td>None</td>
<td>Custom Field - 6</td>
</tr>
<tr>
<td>HTTP_Req_Reference</td>
<td>String</td>
<td>None</td>
<td>Custom Field - 4</td>
</tr>
<tr>
<td>HTTP_Req_URL</td>
<td>String</td>
<td>None</td>
<td>Custom Field - 2</td>
</tr>
<tr>
<td>HTTP_Resp_Length</td>
<td>Unsigned Integer</td>
<td>None</td>
<td>Custom Field - 5</td>
</tr>
<tr>
<td>HTTP_Resp_Status</td>
<td>Unsigned Integer</td>
<td>None</td>
<td>Custom Field - 4</td>
</tr>
<tr>
<td>HTTP_Resp_TTFB</td>
<td>Unsigned Integer</td>
<td>None</td>
<td>Custom Field - 6</td>
</tr>
<tr>
<td>HTTP_Resp_TTLB</td>
<td>Unsigned Integer</td>
<td>None</td>
<td>Custom Field - 7</td>
</tr>
<tr>
<td>HTTP_User_Agent</td>
<td>String</td>
<td>None</td>
<td>Custom Field - 7</td>
</tr>
<tr>
<td>Interface</td>
<td>String</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>Job_Name</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>Language</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>Local_User_Name</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>Message_Text</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Name</td>
<td>Data type</td>
<td>Event field</td>
<td>Flow field</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Method</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>Nat_Details</td>
<td>Custom</td>
<td>Custom Field - 9</td>
<td>Custom Field - 1</td>
</tr>
<tr>
<td>• NAT_Address</td>
<td>IPv4 Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NAT_Port</td>
<td>Unsigned Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NAT_Type</td>
<td>Unsigned Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network_Layer</td>
<td>Signature ID</td>
<td>None</td>
<td>Custom Field - 1</td>
</tr>
<tr>
<td>NTP_Client_Mode</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>NTP_Offset_To_Monitor</td>
<td>Unsigned Integer</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>NTP_Opcode</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>NTP_Request</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>NTP_Server_Mode</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>Num_Copies</td>
<td>Unsigned Integer</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>Object</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>Object_Type</td>
<td>String</td>
<td>Custom Field - 2</td>
<td>None</td>
</tr>
<tr>
<td>Priority</td>
<td>Unsigned Integer</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>Query_Response</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Referer</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>Response Time</td>
<td>Custom</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>• Seconds</td>
<td>Unsigned Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Milliseconds</td>
<td>Unsigned Integer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTMP_Application</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Session_Layer</td>
<td>String</td>
<td>None</td>
<td>Custom Field - 3</td>
</tr>
<tr>
<td>SNMP_Error_Code</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>SNMP_Item</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>SNMP_Item_Type</td>
<td>String</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>SNMP_Operation</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>SNMP_Version</td>
<td>String</td>
<td>Custom Field - 9</td>
<td>None</td>
</tr>
<tr>
<td>Source User</td>
<td>String</td>
<td>Custom Field - 7</td>
<td></td>
</tr>
<tr>
<td>Start_Page</td>
<td>Unsigned Integer</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>Subject</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
<tr>
<td>SWF_URL</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>TC_URL</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>To</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>Transport_Layer</td>
<td>Signature ID</td>
<td>None</td>
<td>Custom Field - 2</td>
</tr>
<tr>
<td>URL</td>
<td>String</td>
<td>Custom Field - 8</td>
<td>None</td>
</tr>
<tr>
<td>User_Agent</td>
<td>String</td>
<td>Custom Field - 6</td>
<td>None</td>
</tr>
<tr>
<td>User_Nickname</td>
<td>String</td>
<td>Custom Field - 5</td>
<td>None</td>
</tr>
<tr>
<td>Version</td>
<td>String</td>
<td>Custom Field - 10</td>
<td>None</td>
</tr>
</tbody>
</table>
Add Time custom types
You can add custom types that enable you to store time data.

Time - Seconds Precision stores time data down to the second. Time - Nanosecond Precision stores time down to the nanosecond. It includes a floating point number with nine precision values representing the nanoseconds.

If you select Index when adding this custom type, the field shows up as a filter on queries, views, and filters. It doesn't appear in distribution components and isn't available in data enrichment, watchlists, or alarms.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, click the Properties icon, then click Custom Types | Add.
2. In the Data Type field, click Time - Seconds Precision or Time - Nanosecond Precision, fill in the remaining information, then click OK.

Name/value custom types
The name/value custom type consists of a group of name/value pairs that you specify. You can filter views and queries by these pairs, and use them in Internal Event Match alarms.

Here are some of the characteristics of this feature:

- The name/value group fields must be filtered using a regular expression.
- They can be correlated so they are selectable in the Correlation rule editor.
- The values part of the pair can only be collected through ASP.
- The maximum size for this custom type is 512 characters, which includes the names. Characters beyond 512 are cut off when collected. McAfee recommends that you limit the size and number of names.
- The names must consist of more than two characters.
- The name/value custom type can have up to 50 names.
- Each name in the name/value group is displayed in the global filter as <name of the group> - <name>.

Add name/value group custom type
If you add a group of name/value pairs, you can filter views and queries by them and use them in Internal Event Match alarms.

Task
For option definitions, click ? in the interface.

1. On the system navigation tree, select the system, then click the Properties icon.
2. Click Custom Types, then click Add.
3. In the Data Type field, click Name/Value Group, fill in the remaining information, then click OK.
Managing cases

Use the ESM case manager to assign and track work items and support tickets associated with network events. To access this feature, you must be part of a group that has the Case Management User privilege enabled.

There are five ways to add a case:

• On the Case Management view
• On the Cases pane, without linking to an event
• On the Event Analysis view, linking it to an event
• When you set up an alarm
• On a triggered alarm notification

Contents

» Add a case
» Create a case from an event
» Add events to an existing case
» Edit or close a case
» View case details
» Add case status levels
» Email cases
» View all cases
» Generate case management reports

Add a case

Your first step in tracking a task generated as the result of a network event is to add a case to the case management system.
Task
For option definitions, click ? in the interface.

1. On the Cases pane, click the Add Case icon.
2. Fill in the information requested, then click OK.

The case is added to the Cases pane of the user the case is assigned to. If you selected Email case, an email is also sent (see Email a case).

Create a case from an event

To track an event on the Event Analysis view, create a case. This enables workflow tracking.

Task
For option definitions, click ? in the interface.

1. On the views list, select Event Views | Event Analysis.
2. Click the event, click the menu icon, then click Actions | Create a new case.
3. Complete the information requested, then click OK to save the case.

The new case includes the event data in the Message table.

Add events to an existing case

Add one or more events to an existing case to keep track of actions taken in response to those events.

Task
For option definitions, click ? in the interface.

1. On the views pane, select Event Views from the view drop-down list, then click Event Analysis.
2. Select the events, then do one of the following:
   • Click the Assign Events to a Case or Remedy icon and select Add events to a case.
   • Click the Menu icon, highlight Actions, then click Add events to a case.
3. Select the case and click Add.

The Case Details page lists the event ID in the Messages table.
4. Click OK, then click Close.

Edit or close a case

If you have Case Management Administrator privileges, you can modify any case on the system. If you have Case Management User privileges, you can modify only cases that are assigned to you.
**Task**
For option definitions, click ? in the interface.

1. Access Case Details in one of these ways.

<table>
<thead>
<tr>
<th>For...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A case assigned to you</td>
<td>1. Select the case on the Cases pane.</td>
</tr>
<tr>
<td></td>
<td>2. Click the Edit Case icon.</td>
</tr>
<tr>
<td>A case not assigned to you</td>
<td>1. Click the Open Case Management icon in the Cases pane.</td>
</tr>
<tr>
<td></td>
<td>2. Select the case to be modified.</td>
</tr>
<tr>
<td></td>
<td>3. Click the Edit Case icon at the bottom of the view.</td>
</tr>
</tbody>
</table>

2. Edit the settings or close the case in the Status field.

3. Click OK to save the changes.

The changes are recorded in the Notes section of the Case Details page. If you closed the case, it no longer appears on the Cases pane, but remains on the Case Management list with the status changed to Closed.

---

**View case details**

If you have Administrator rights on the ESM you can view and take action on any case on the ESM. All the users in a group can view any case in their group.

**Task**
For option definitions, click ? in the interface.

1. On the Cases pane, click the Open Case Management icon.

The Case Management view opens, listing all cases on the system.

2. Review the data on the Notes and Source Events tabs.

3. For further details, double-click the case, then review the information on the Case Details page.

---

**Add case status levels**

The case manager comes with two status levels: Open and Closed. You can add other statuses that cases can be assigned to.

**Task**
For option definitions, click ? in the interface.

1. On the Cases pane, click the Open Case Management icon.

2. On the Case Management view, click the Case Management Settings icon on the bottom toolbar, then click Add.
3 Type a name for the status, then select if you want this status to be the default for new cases.

4 Select if you want cases with this status to be shown in the Cases pane, then click OK.

**Email cases**

Set the system to automatically send an email message to the person or group a case is assigned to, every time a case is added or reassigned.

**Before you begin**

You must have Case Management Administrator privileges.

You can also email a case notification manually, and include case notes and event details.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email a case automatically</td>
<td>1 On the Cases pane, click the Open Case Management icon.</td>
</tr>
<tr>
<td></td>
<td>2 Click the Case Management Settings icon.</td>
</tr>
<tr>
<td></td>
<td>3 Select Send an email when a case is assigned, then click Close.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Info" /> Email addresses for the users must be on the ESM (see Setup users).</td>
</tr>
</tbody>
</table>

| Email an existing case manually      | 1 On the Cases pane, select the case you want to email, then click the Edit Case icon.        |
|                                      | 2 On Case Details, click Email Case, then fill in the From and To fields.                     |
|                                      | 3 Select whether you want to include the notes and attach a CSV file of the event details.   |
|                                      | 4 Type any notes you want to include in the email message, then click Send.                   |

**View all cases**

If you have Administrative privileges on the ESM, you can manage all cases on the system, whether they are currently open or closed. Case Management Administrator privileges give you the ability to create statuses, organizations, and set the automatic email functionality.

**Task**

For option definitions, click ? in the interface.

1 On the Cases pane, click the Open Case Management icon.

The Case Management view open.
2 Do any of the following:

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a case</td>
<td>Click the Add Case icon on the toolbar at the bottom of the view.</td>
</tr>
<tr>
<td>View or edit the selected case</td>
<td>Click the Edit Case icon on the toolbar at the bottom of the view.</td>
</tr>
<tr>
<td>Email the selected case</td>
<td>Click the Email Case icon on the toolbar at the bottom of the view.</td>
</tr>
<tr>
<td>Set a case up to send an email when a case is added or changed</td>
<td>Click the Case Management Settings icon on the toolbar at the bottom of the view.</td>
</tr>
<tr>
<td>Add or edit the statuses available for cases</td>
<td>Click the Case Management Settings icon and click Add, Edit, or Delete.</td>
</tr>
<tr>
<td>View the notes, history, and source events for the case you select</td>
<td>Click Notes, History, or Source Events. When you click Source Events, the Source Event details tabs open. If the tabs aren’t visible or if they are visible and you want to hide them, click the View Source Event details icon on the toolbar at the bottom of the view. The History tab records any time a user views a case. If the same user views a case more than once within five minutes, it doesn’t update the record each time.</td>
</tr>
<tr>
<td>Filter the cases</td>
<td>On the Filters pane, select or type the data you want to filter the cases by, then click the Run Query icon. The list of cases changes to show only the ones that meet the filter criteria.</td>
</tr>
</tbody>
</table>

### Generate case management reports

There are six case management reports available on the ESM.

**Task**

For option definitions, click ? in the interface.

1. On the System Properties page, click Reports | Add.
2. Complete sections 1, 2, and 3.
3. In section 4, select Query CSV.
4. In section 5, select the case management report to run.

- **Case Management Summary** — Includes case ID numbers, the severity assigned to the cases, their status, the users they are assigned to, the organizations where they are assigned (if any), the date and time that the cases were added, the date and time that the cases were updated (if they have been), and the case summaries.

- **Case Management Details** — Includes all information in the Case Management Summary report as well as the ID numbers of the events linked to the cases and the information included in the notes sections of the cases.

- **Case Time to Resolution** — Shows the length of time that it took between status changes (for example, the differential between the Open time stamp and Closed time stamp). By default, it lists the cases with a status of Closed by Case ID number as well as severity, organization, Created date, last update, summary, and time difference.

- **Cases per Assignee** — Includes the number of cases assigned to a user or group.
• **Cases per Organization** — Includes the number of cases per organization.

• **Cases per Status** — Includes the number of cases per status type.

5. Complete section 6 (see *Description of contain and regex filters*), then click **Save**.

The report is saved and added to the **Reports** list.
Working with the Asset Manager

The Asset Manager provides a centralized location that allows you to discover, manually create, and import assets.

On the Asset tab, 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 the group.
  
  **This change is not persistent. If you add an asset to a changed group, it will not automatically inherit the previous settings.**

- Use drag and drop operations.
- Rename a group if necessary.

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.

There are two ways that the tags of an asset can be defined: by the system when an asset is retrieved or by the user when an asset is added or edited. 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 will not update the tag when the asset is retrieved, even if they have changed. If you add or edit the tags of an asset but you want the system to update them when the asset is retrieved, click **Reset**. You must complete this action each time you change the tag settings.

Configuration management is part of standard compliance regulations such as PCI, HIPPA, and SOX. It allows you to monitor any changes that might be made to the configuration of your routers and switches, thus preventing system vulnerabilities. On the ESM, the configuration management feature enables you to:

- Set the frequency with which devices must be polled.
- Select the discovered devices on which to check configuration.
- Identify a retrieved configuration file as the default for the device.
- View the configuration data, download the data to a file, and compare the configuration information of the two devices.
Manage assets

An asset is any device on the network that has an IP address.

On the Asset tab of the Asset Manager, you can create assets, modify their tags, create asset groups, add asset sources, and assign an asset to an asset group. You can also manipulate the assets that are learned from one of the vulnerability assessment vendors.

Task

For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon.
2. Make sure the Asset tab is selected.
3. Manage the assets as needed, then click OK.

Tasks

- Define old assets on page 274

The Old Assets group on the Asset Manager allows you to store assets that haven’t been detected in the period of time that you define.

Define old assets

The Old Assets group on the Asset Manager allows you to store assets that haven't been detected in the period of time that you define.

Task

For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon.
2. On the Asset tab, double-click the Old Assets group on 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.
Set up configuration management

Configuration management retrieves the configuration files of devices that have been successfully discovered using the CLI profile. Once the network discovery process is completed, you must set up configuration management.

Task

For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then select the Configuration Management tab.

2. Perform any of the available actions, then click OK.

Tasks

- Manage retrieved configuration files on page 275
  - There are several things you can do to manage the files that are retrieved when the configuration of your routers and switches is checked.

Manage retrieved configuration files

There are several things you can do to manage the files that are retrieved when the configuration of your routers and switches is checked.

Before you begin

Retrieve configuration files (see Set up configuration management).

Task

For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then select the Configuration Management tab.

2. Perform any of the available actions in the Retrieved configuration files section of the page.

Network Discovery

Network Discovery shows the physical locations where events have occurred on your network, increasing your ability to track down events.

Network Discovery is for advanced users with extensive network knowledge and is an assigned privilege only. You must have privileges enabled to create and view Network Discovery and modify the switch settings on Network Port Control.

- Network Discovery from SNMPv3, Telnet, or SSH is not FIPS-compliant. If you are required to comply with FIPS regulations, do not use these features.

Discover the network

The first step in mapping your network is discovering the network. You must set the parameters before initiating the scan.
**Task**  
For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then select the Network Discovery tab.
2. Click Settings, then click Add on the Configure Network Settings page to add the parameters for this discovery.
3. Complete the Network Discovery Parameters settings.
4. Click OK. The parameters you defined are added to the Configure Network Settings list.
5. Perform other actions as needed.
6. Click Discover Network to initiate the scan. If you must stop the discovery, click Stop Discovery.
   The Network Device section of the page is populated with the data from the scan.
7. Click OK.

**Manage the IP exclusion list**  
You can add IP addresses to the IP Exclusion List if you want to exclude them from the network discovery search.

**Task**  
For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then select the Network Discovery tab.
2. Click IP Exclusion list.
3. Add a new address, edit, or remove an existing one.
4. Click OK to save your changes.

**Discover endpoints**  
When you set up your network, add IP addresses to the exclusion list, and discover your network, you must discover endpoints connected to your devices.

**Task**  
For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then select the Network Discovery tab.
2. Click Discover Endpoint to initiate the scan now.
   The results and status of the scan are listed in the Endpoint Devices section of the page.
3. To schedule auto discovery of the endpoints, select Auto discover every and select the frequency.

**View a map of the network**  
You can generate a graphical representation of your network that allows you to maneuver the devices to any position.
**Task**
For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then click the Network Discovery tab.

2. Click Network Map.
   - The graphical representation of your network opens.

3. Move devices or roll your mouse over a device to view its properties.

**Change Network Discovery behavior**
You can change the default ping, number of end station, and concurrent devices settings of Network Discovery.

**Task**
For option definitions, click ? in the interface.

1. On the ESM console, click the Asset Manager quick launch icon.

2. Click the Network Discovery tab, click Settings, then click Advanced.

3. Change the settings as needed, then click OK.

---

**Asset Sources**
You can retrieve data from your Active Directory, if you have one, or an Altiris server using Asset Sources. Active Directory allows you to filter event data by selecting the retrieved users or groups in the Source User or Destination User view query filter fields. This improves your ability to provide compliance data for requirements like PCI. Altiris and Active Directory retrieve assets such as computers with IP addresses, and add them to the assets table.

In order to retrieve assets on Altiris, you must have Asset Manager privileges on the Altiris Management Console.

Active Directory doesn’t typically store IP address information. The system uses DNS to query for the address once it gets the name from Active Directory. If it can’t find the address of the computer, it doesn’t get added to the Assets table. For this reason, the DNS server on the system needs to contain the DNS information for Active Directory computers.

You can add IP addresses to Active Directory. If you do this, modify the `networkAddress` attribute on your computer objects so the system uses those IP addresses instead of querying DNS.

**Manage asset sources**
Retrieve data from your Active Directory or an Altiris server.
Task
For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then click the Asset Sources tab. The Asset Sources tree shows the ESM and Receivers on the system, and their current asset sources.

   An ESM can have one and Receivers can have multiple asset sources.

2. Select a device then select either of the available actions.

Manage vulnerability assessment sources
You can retrieve data from a variety of VA vendors using Vulnerability Assessment. To communicate with the desired VA sources, you must add the source to the system. Once a source is added to the system, you can retrieve the VA data.

Task
For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then click the Vulnerability Assessment tab.

2. Add, edit, remove, or retrieve VA sources, then write them to the device.

3. Click OK.

Zone Management
Zones can be used to categorize devices and data sources on your network. This enables you to organize devices and the events they generate into related groupings by geographic location and IP address. For example, if you have offices on the East Coast and the West Coast and you want the events generated by each office to be grouped together, you add two zones and assign the devices whose events must be grouped to each of the zones. To group the events from each office by specific IP addresses, you add subzones to each of the zones.

Manage zones
Zones help you categorize your devices and data sources by geolocation or ASN. You must add zones, either individually or importing a file exported from another machine, and assign the devices or data sources to the zones.

Task
For option definitions, click ? in the interface.

1. Click the Asset Manager quick launch icon, then select Zone Management.

2. Add a zone or subzone, edit or remove existing zones, or import or export zone settings.

3. Rollout any changes you make, then click OK.
Add a zone
The first step in zone management is to add the zones used to categorize your devices and data sources. They can be added individually using the Add Zone feature or you can import a file that was exported from another system. When a zone is added, you can edit its settings when required.

Task
For option definitions, click ? in the interface.

1 Click the Asset Manager quick launch icon , then click Zone Management.
2 Enter the information requested and assign devices to the zone, then click OK.

Export zone settings
You can export the zone settings from your ESM so you can import them to another ESM.

Task
For option definitions, click ? in the interface.

1 Click the Asset Manager icon , then click Zone Management.
2 Click Export, then select the type of file you want to export.
3 Click OK and select the file to download now.

Import zone settings
This import feature allows you to import a zone file as is, or edit the data before importing it.

Before you begin
Export a file of zone settings from another ESM so that it can be imported to your ESM.

Task
For option definitions, click ? in the interface.

1 Open the zone settings file that you want to import.
   • If this file is an import zone definition file, it has eight columns: Command, Zone Name, Parent Name, Geo Location, ASN, Default, IPStart, and IPStop.
   • If it is an import device to zone assignment file, it has three columns: Command, Device Name, and Zone Name.

2 Enter commands in the Command column to specify the action to be taken for each line when it is imported.
   • add — Import the data in the line as it is.
   • edit — (Zone definition file only) Import the data with any changes you make to the data.
   • remove — Delete the zone matching this line from the ESM.
3 Save the changes you made, then close the file.
4 Click the Asset Manager quick launch icon, then click the Zone Management tab.

5 Click Import, then select the type of import it will be.

6 Click OK, then locate the file to be imported and click Upload. The system notifies you if errors are detected in the file.

7 If there are errors, make the necessary corrections to the file and try again.

8 Roll out the changes to update the devices.

Add a subzone
Once you have added a zone, you can add subzones to further categorize the devices and events by IP address.

Before you begin
Add zones on the Zones Management tab.

Task
For option definitions, click ? in the interface.

1 Click the Asset Manager quick launch icon, then click the Zone Management tab.

2 Select a zone, then click Add Sub-zone.

3 Fill in the information requested, then click OK.

Asset, threat, and risk assessment
McAfee Threat Intelligence Services (MTIS) and the vulnerability assessment sources on your system generate a list of known threats. The severity of these threats and the criticality of each of your assets are used to calculate the level of risk to your enterprise.

Asset Manager
When you add an asset to your Asset Manager (see Manage assets), you assign a criticality level. This setting represents how critical the asset is to your operation. For example, if you have one computer managing your enterprise setup and it doesn't have a backup, its criticality is high. If, however, you have two computers managing your setup, each with a backup, the criticality level is considerably lower.

You can select whether to use or ignore an asset in risk calculation for your enterprise on the Edit menu of the Asset tab.

Threat Management
The Threat Management tab on the Asset Manager shows a list of known threats, their severity, the vendor, and whether they are used when calculating risk. You can enable or disable specific threats so that they are or are not used to calculate risk. You can also view the details for the threats on the list. These details include recommendations for dealing with the threat as well as countermeasures you can use.
Pre-defined views
Three pre-defined views (see Working with ESM views) summarize and display asset, threat, and risk data:

- **Asset threat summary** — Displays the top assets by risk score and threat levels, and threat levels by risk.
- **Recent threat summary** — Displays recent threats by vendor, risk, asset, and available protection products.
- **Vulnerability summary** — Displays vulnerabilities by threats and assets.

Details of individual items on these views can be accessed from the component menus.

Custom views
Options have been added to the Query Wizard to enable you to set up custom views (see Add a custom view) that display the data you need.

- On the Dial Control and Count components, you can display the average enterprise risk score and the total enterprise risk score.
- On the Pie Chart, Bar Chart, and List components, you can display the assets at risk, product threat protection, threat by asset, threat by risk, and threat by vendor.
- On the Table component, you can display assets, most recent threats, top assets by risk score, and top threats by risk score.

Manage known threats
Select which known threats to use in risk calculations.

Each threat has a severity rating. This rating and the criticality rating for your assets are used to calculate the overall severity of a threat to your system.

**Task**
For option definitions, click ? in the interface.

1. On the ESM console, click the Asset Manager quick launch icon.

2. Click the Threat Management tab to display the list of known threats.

3. Select a known threat, then do one of the following:
   - Click Threat Details to view the details about the threat.
   - If the Calculate Risk column says Yes and you do not want it to be used in risk calculations, click Disable.
   - If the Calculate Risk column says No, and you want it to be used in risk calculations, click Enable.

4. Click OK.
Managing policies and rules

Create, apply, and view policy templates and rules.

Contents
- Understanding the Policy Editor
- The Policy Tree
- Rule types and their properties
- Default Policy settings
- Rule operations
- Assign tags to rules or assets
- Modify aggregation settings
- Override action on downloaded rules
- Severity weights
- View policy change history
- Apply policy changes
- Manage priority traffic

Understanding the Policy Editor

The Policy Editor allows you to create policy templates and customize individual policies. Policy templates, as well as policy settings on any device, can inherit values from their parents. Inheritance allows policy settings applied to a device to be infinitely configurable while maintaining a level of simplicity and ease-of-use. Each policy that is added, with all devices, has an entry in the Policy Tree.

⚠️ When operating in FIPS mode, do not update rules through the rule server. Instead, update them manually (see Check for rule updates).

The McAfee rule server maintains all rules, variables, and preprocessors with predefined values or usages. The Default Policy inherits its values and settings from these McAfee-maintained settings, and is the ancestor of all other policies. Settings for all other policies and devices inherit their values from the Default Policy by default.
To open the editor, click the **Policy Editor** icon, or select the system or device node in the navigation tree and click the **Policy Editor** icon in the actions toolbar.

The types of rules listed in the **Rule Types** pane vary based on the type of device selected in the system navigation tree. The bread crumb navigation pane displays the hierarchy of the policy you have selected. To change the current policy, click the policy's name on the bread crumb navigator pane and click the arrow in the bread crumb navigator pane, which displays the children of the policy. Or, click the **Policy Tree** icon. The menu on the **Policy Tree** lists the things you can do to a policy.

When you select a type in the **Rule Type** pane, all rules of that type are listed in the rule display section. The columns list the specific rule parameters that you can adjust for each rule (except for **Variable** and **Preprocessor**). You can change the settings by clicking the current setting and selecting a new one from the drop-down list.

The **Filters/Tagging** pane filters rules displayed in the **Policy Editor** so that you can view only those that meet your criteria, or add tags to the rules to define their functions.

---

**The Policy Tree**

The **Policy Tree** lists the policies and devices on the system.

The **Policy Tree** allows you to:
• Navigate to view the details of a specific policy or device
• Add a policy to the system
• Modify the order of the policies or devices
• Locate any policy or device by name
• Rename, delete, copy or copy and replace, import, or export a policy

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td></td>
</tr>
<tr>
<td>Device is out of sync</td>
<td></td>
</tr>
<tr>
<td>Device is staged</td>
<td></td>
</tr>
<tr>
<td>Device is up-to-date</td>
<td></td>
</tr>
<tr>
<td>Virtual Device is out of sync</td>
<td></td>
</tr>
<tr>
<td>Virtual Device is staged</td>
<td></td>
</tr>
<tr>
<td>Virtual Device is up-to-date</td>
<td></td>
</tr>
<tr>
<td>Data Source is out of sync</td>
<td></td>
</tr>
<tr>
<td>Data Source is staged</td>
<td></td>
</tr>
<tr>
<td>Data Source is up-to-date</td>
<td></td>
</tr>
<tr>
<td>ADM is out of sync</td>
<td></td>
</tr>
<tr>
<td>DEM is out of sync</td>
<td></td>
</tr>
</tbody>
</table>

**Manage policies on the Policy Tree**

Manage the policies on the system by taking actions on the Policy Tree.

**Task**

For option definitions, click ? in the interface.

1. On the ESM console, click the Policy Editor icon , then click the Policy Tree icon .

2. Do any of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the rules of a policy</td>
<td>• Double-click the policy. The rules are listed in the rule display section of the Policy Editor.</td>
</tr>
<tr>
<td>Make a policy the child of another</td>
<td>• Select the child, then drag-and-drop it on the parent.</td>
</tr>
<tr>
<td></td>
<td>• You can only drag-and-drop devices onto policies.</td>
</tr>
<tr>
<td>Locate a policy or device</td>
<td>• Type the name in the search field.</td>
</tr>
<tr>
<td>Add a new policy</td>
<td>1 Select the policy that you want to add a new policy to, then click the Policy Tree Menu Items icon .</td>
</tr>
<tr>
<td></td>
<td>2 Click New, enter a name for the policy, then click OK.</td>
</tr>
</tbody>
</table>
To... | Do this...
---|---
**Rename a policy** | 1 Select the policy you want to rename, then click the **Policy Tree Menu Items** icon.  
2 Click **Rename**, enter the new name, then click **OK**.

**Delete a policy** | 1 Select the policy you want to delete, then click the **Policy Tree Menu Items** icon.  
2 Click **Delete**, then click **OK** on the confirmation page.

**Copy a policy** | 1 Select the policy you want to copy, then click the **Policy Tree Menu Items** icon.  
2 Click **Copy**, enter a name for the new policy, then click **OK**.

**Move devices to a policy** | 1 Select the devices that you need to move, then click the **Policy Tree Menu Items** icon.  
2 Highlight **Move**, then select the policy you want to move the devices to.

**Copy and replace a policy** | 1 Select the policy you want to copy, click the **Policy Tree Menu Items** icon, then select **Copy and Replace**.  
2 In **Select Policy**, select the policy you want to replace.  
3 Click **OK**, then click **Yes**.  
The settings of the policy you copied are applied to the policy you replaced, but the name remains the same.

**Import a policy** | The import occurs from the currently selected device down.  
1 Select the level on the tree where you want to import the new policy, click the **Policy Tree Menu Items** icon, then select **Import**.  
2 Browse to and upload the file you want to import.  
3 If an error message appears, see **Troubleshoot Import Policy** for a solution.  
3 Select the import options that you want to use, then click **OK**.

**Export a policy** | 1 Select the policy that you want to export.  
The export includes the selected node and up in the hierarchy. Only standard rules with custom settings or custom rules are exported, so at least one of these must be selected for the **Export** option to enable.  
2 Click **Menu**, then select **Export**.  
3 Select the export options you want to use, click **OK**, then select the location to save the exported policy file.

3 To close the **Policy Tree**, double-click a policy or device, or click the close icon 📌.

---

**Rule types and their properties**

The **Rule Types** pane of the **Policy Editor** page allows you to access all rules by type.  
You can import, export, add, edit, and perform various operations on a rule once it is selected. The functions that you can perform are limited by the type of rule.
All rules are based on a hierarchy system in which each rule inherits its usage from its parent. The rule (except for Variable and Preprocessor rules) is marked with an icon to indicate where it inherits its usage, and the icon has a dot on the lower-left corner if the inheritance chain broke somewhere below the current row.

### Icon Description

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon 1" /></td>
<td>Indicates that the usage for this item is determined by the parent’s setting. Most rules are set to inherit by default, but the usage can be changed.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon 2" /></td>
<td>Indicates that the inheritance chain is broken at this level and the inheritance value is turned off. The current rule usage is used when the inheritance chain is broken.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon 3" /></td>
<td>Indicates that the inheritance chain is broken at this level. Items below this point do not inherit any further up the chain. This setting is useful to force rules to use their default.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon 4" /></td>
<td>Indicates a custom value; you set the value to something other than the default.</td>
</tr>
</tbody>
</table>

### Properties

When a rule type is selected, the rule display pane shows all rules of that type on the system and their property settings. These properties can include Action, Severity, Blacklist, Aggregation, and Copy Packet.

<table>
<thead>
<tr>
<th>This property...</th>
<th>Allows you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Set the action performed by this rule. The available options are based on the type of rule. Blacklist items can’t move on to their destination; if Pass is selected in the Blacklist column, the system automatically changes it to Alert.</td>
</tr>
<tr>
<td>Severity</td>
<td>Select the severity of the rule portion when the rule is triggered. Severity is based on 1 to 100, with 100 being the most severe.</td>
</tr>
<tr>
<td>Blacklist</td>
<td>Auto-create a blacklist entry on a per rule basis when the rule is triggered on the device. You can choose whether to blacklist only the IP address or the IP address and port.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Set per rule aggregation for events that are created when a rule is triggered. The aggregation settings defined on the Event Aggregation pages (see Aggregate events or flows) apply only to those rules that are set in the Policy Editor.</td>
</tr>
<tr>
<td>Copy Packet</td>
<td>Copy packet data to the ESM, which is useful in the event of lost communication. If there is a copy of the packet data, you can access the information by retrieving the copy.</td>
</tr>
</tbody>
</table>

Change these settings by clicking the current setting and selecting another.

### Variables

A **variable** is a global setting or a placeholder for information that is user- or site-specific. Many rules use variables.

We recommend that you have extensive knowledge of Snort format before adding or modifying variables.
Variables are used to make rules behave in a specific way, which might vary from device to device. The ESM has many pre-set variables, but also provides the ability to add custom variables. When adding a rule, these variables appear as options in the drop-down list for the field type selected in the Type field on the New Variable page.

Each variable has a default value, but we recommend that you set some values that correspond to the specific environment of each device. No spaces are allowed when entering a variable name. If a space is necessary, use the underscore ( _ ) character. To maximize the effectiveness of a device, it is particularly important to set the HOME_NET variable to the home network being protected by the specific device.

This table shows a list of common variables and their default values.

<table>
<thead>
<tr>
<th>Variable names</th>
<th>Description</th>
<th>Default</th>
<th>Default description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXTERNAL_NET</td>
<td>Everyone outside of the protected network</td>
<td>!$HOME_NET</td>
<td>Port 80</td>
</tr>
<tr>
<td>HOME_NET</td>
<td>Local protected network address space: (10.0.0.0/80)</td>
<td>Any</td>
<td>Same as HOME_NET</td>
</tr>
<tr>
<td>HTTP_PORTS</td>
<td>Web server ports: 80 or 80:90 for a range between 80 and 90</td>
<td>80</td>
<td>Any port except the HTTP_PORTS</td>
</tr>
<tr>
<td>HTTP_SERVRS</td>
<td>Addresses of web servers: 192.168.15.4 or [192.168.15.4,172.16.61.5]</td>
<td>$HOME_NET</td>
<td>Same as HOME_NET</td>
</tr>
<tr>
<td>SHELLCODE_PORTS</td>
<td>Anything but web server ports</td>
<td>!$HTTP_PORTS</td>
<td>Same as HOME_NET</td>
</tr>
<tr>
<td>SMTP</td>
<td>Mail server addresses</td>
<td>$HOME_NET</td>
<td>Same as HOME_NET</td>
</tr>
<tr>
<td>SMTP_SERVERS</td>
<td>Mail server addresses</td>
<td>$HOME_NET</td>
<td>Same as HOME_NET</td>
</tr>
<tr>
<td>SQL_SERVERS</td>
<td>Addresses of SQL DB servers</td>
<td>$HOME_NET</td>
<td>Same as HOME_NET</td>
</tr>
<tr>
<td>TELNET_SERVERS</td>
<td>Addresses of telnet servers</td>
<td>$HOME_NET</td>
<td>Same as HOME_NET</td>
</tr>
</tbody>
</table>

Variables that come with the system can be modified. Custom variables can be added, modified, or deleted.

You can assign types to custom variables. Variable types are used when filtering rules for reporting and they determine the field in which the variables are available when adding or modifying a rule. Variable types are global in nature, and any changes that are made are reflected on all levels of the policy.

Manage variables

When you select the variable rule type on the Policy Editor, you can take several actions to manage both custom and predefined variables.

Task

For option definitions, click ? in the interface.

1. Click the Policy Editor icon.
2. On the Rule Types pane, select Variable.
3. Do any of the following:
To... | Do this...
--- | ---
Add a new category | 1 Select New | Category.  
2 Enter a name for the new category, then click OK.
Add a custom variable | 1 In the rules display pane, select the category, then click New.  
2 Select Variable, then define the requested settings.  
3 Click OK.
Modify a variable | 1 In the rules display pane, select the variable to be modified.  
2 Select Edit, then click Modify.  
3 Modify the value or description, then click OK.
Delete a custom variable | 1 In the rules display pane, select the variable to be removed.  
2 Select Edit, then click Delete.
Import a variable | 1 Select File, then click Import | Variables.  
2 Click Import, then browse and upload the file.  
**Note:** The import file must be a .txt file containing the following information in this format: VariableName;VariableValue; CategoryName (optional); Description (optional). If one field is missing, a semi-colon must be in place to act as a place holder.
Modify the type of custom variable | 1 Select the custom variable.  
2 Click Edit, then select Modify.  
3 Change the variable type.  
**Note:** When the variable type is set to something other than No Type Selected and committed, you can’t change the value.  
4 Click OK to save changes.

### Detect TCP protocol anomalies and session hijacking

You can detect and alert on TCP protocol anomalies and check to TCP session hijacking using the Stream5 preprocessor variable.

**Task**
For option definitions, click ? in the interface.

1. On the ESM console, click the Policy Editor icon.
2. In the Rule Types pane, click Variable.
3. In the rules display pane, click preprocessor, then select STREAM5_TCP_PARAMS.
4. On the Modify Variable page, add one of the following in the Value field:
   - To detect and alert on TCP protocol anomalies, add detect_anomalies after policy first.
   - To check for TCP session hijacking, add detect_anomalies check_session_hijacking after policy first.
Preprocessor rules

Preprocessors provide a way to unify anomaly detection and packet inspection in the McAfee Nitro IPS and IDS.

Preprocessors are vital to the accurate detection of many rules. Use the preprocessors that apply to your network configuration. Parameters for the preprocessors can be changed by editing the respective preprocessor variable under the Variables rule type in the Policy Editor.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC Normalization</td>
<td>Normalizes RPC protocol-specific traffic into a uniform way for detection purposes only. This preprocessor can prevent RPC fragmentation-related attacks from bypassing the Nitro IPS.</td>
</tr>
<tr>
<td>Portscan Detection</td>
<td>Generates an event if it detects a Portscan on the devices on the trusted side of your network.</td>
</tr>
<tr>
<td></td>
<td>Once you have correctly set the HOME_NET variable, you should modify the variable SFPORTSCAN_PARMS (Variables</td>
</tr>
<tr>
<td></td>
<td>proto { all } scan_type { all } sense_level { medium } ignore_scanners</td>
</tr>
<tr>
<td></td>
<td>This is added to the sfportscan variable to eliminate what the Nitro IPS recognizes are port scans from the HOME_NET. Networks that place the Nitro IPS or IDS near a router or firewall that does Network Address Translation (NAT) appear to be portscanning to the Nitro IPS. Modifying the variable reduces what looks like false positive events.</td>
</tr>
<tr>
<td></td>
<td>HOME_NET can't be set to “any” for ignore_scanners to work properly.</td>
</tr>
<tr>
<td>ZipZap</td>
<td>When serving web (HTTP) content, many web servers accept requests from web browsers, indicating that the web content can be compressed before it is sent. While this saves network bandwidth, compressed webpages cannot be analyzed by a device. The ZipZap preprocessor causes the web server to return this data in a raw, uncompressed and analyzable format. Enabling this preprocessor increases the amount of bandwidth used by web traffic.</td>
</tr>
<tr>
<td>Target-based IP Defragmenter</td>
<td>Models the actual targets on the network instead of merely modeling the protocols and looking for attacks within them. It uses the sfxhash data structure and linked lists for data handling internally, allowing it to have predictable and deterministic performance in any environment, which aids in managing heavily fragmented environments.</td>
</tr>
<tr>
<td>Web Request Normalization</td>
<td>Normalizes web requests into a uniform way for detection purposes only. It's always enabled; however, you are not allowed to make changes. There are two types of Web Request Normalization preprocessors, one for use with versions up to 8.2.x and the other for 8.3.0 and later.</td>
</tr>
<tr>
<td></td>
<td>This preprocessor detects these attacks:</td>
</tr>
<tr>
<td></td>
<td>• Web directory traversal attacks (<a href="http://something.com/./attack.cmd">http://something.com/./attack.cmd</a>)</td>
</tr>
<tr>
<td></td>
<td>• Double-encoded strings (<a href="http://something.com/%25%32%35%25%33%32%25%33%30attack.cmd">http://something.com/%25%32%35%25%33%32%25%33%30attack.cmd</a>)</td>
</tr>
<tr>
<td></td>
<td>• Unicode normalization</td>
</tr>
<tr>
<td></td>
<td>• Invalid characters in a web request URI</td>
</tr>
<tr>
<td>Target-based TCP Reassembly and TCP/UDP Session Tracking</td>
<td>Tracks sessions. It is a Stream5 preprocessor so the rule flow and flow bits keywords are usable with TCP and UDP traffic.</td>
</tr>
</tbody>
</table>

Manage preprocessor rules

Turn each preprocessor on or off, and set its inheritance.
Task
For option definitions, click ? in the interface.

1. In the Rule Types pane on the Policy Editor, click IPS | Preprocessor.
2. Select Inherit, On, or Off for the active rules.

Firewall rules
Firewall rules are used to detect network events based on packet information such as protocol, port, or IP address on a Nitro IPS.

The firewall policy scans incoming packets and makes decisions based on initial information found before the packet is passed to the deep packet inspection engine. Firewall rules will block things like spoofed and invalid IP addresses. They also track the rate and size of network traffic.

These are the types of firewall rules:

- **Anomaly** — Detects anomalies. Many anomaly-based rules coincide with one another and are used with the values set in the Variables tab. For example, the rule Long Connection Duration and the variable Long Duration Seconds are used together to determine the number of seconds before the rule is triggered. To see more specific details on each rule, look at the detail section, located at the bottom of the page.

- **Anti-Spoof** — Detects invalid IP addresses. For example, if a reserved internal IP address is seen entering the network through a device, the anti-spoof rule is triggered.

- **Blacklist** — Determines the action to be taken on packets that are being sent to or from a blacklisted IP address or port.

- **DHCP** — Turns on and off the capability to allow DHCP traffic through a device.

- **IPv6** — Detects IPv6 traffic.

- **Port-Block** — Blocks certain ports.

Anomaly detection
Certain firewall rules are rate-based. A rate-based rule is a rule that only triggers an alert if your network traffic exceeds the thresholds defined by firewall-category variables in the Policy Editor. The default values for these variables might not make sense for your network's traffic, so the Rate-Based Anomaly Detection Wizard provides the ability to analyze graphs of your network flow data as it relates to these parameters (see Anomaly Detection wizard).

Firewall exceptions
Firewall exceptions are sometimes necessary to allow certain types of traffic to pass through the firewall that would otherwise be blocked. For example, if a valid internal address comes from the outside network, such as a VPN, it triggers an Incoming Bogons alert. To stop the alert, you must set up an exception to the firewall rule.

You can also select to treat an exception as an exception to the patterns defined in other exceptions, creating an exception to the exception list (in other words, include an address or block of addresses). If an address needs to be checked against a firewall rule and the IP address is in a block of addresses that has already been accepted, it can be excluded from the exception list by entering the IP address (or mask) and selecting the box.
As an example, the exception list already contains the block of addresses 10.0.0.0/24. All addresses in this range are an exception to the rule. If the source address 10.0.0.1 is active for this rule, select **Treat this as an exception to the patterns defined in other exceptions** and type 10.0.0.1 in the source field. The firewall rule then applies to 10.0.0.1, but not to any other address in the 10.0.0.0/24 block, because 10.0.0.1 is now the exception to the exception list.

**Add a custom firewall rule**

Typically, the default firewall rules are sufficient to protect the network. However, there might be an occasion where you need to add rules specific to a protected system or environment.

**Task**

For option definitions, click ? in the interface.

1. In the **Rule Types** pane of the **Policy Editor**, select **IPS | Firewall**.
2. Select **New**, then click **Firewall Rule**.
3. Define the settings, then click **OK**.

The filters in the new rule are applied and the new rule appears in the rule display pane. If you click the filter icon  filtro, the filtering is cleared.

**Add firewall exceptions**

Add exceptions to firewall rules to allow network events from specified protocols, IP addresses, or ports to pass through the firewall.

**Task**

For option definitions, click ? in the interface.

1. On the **Policy Editor**, select **IPS | Firewall**.
2. In the rule display pane, click the rule that you want to add an exception to.

   For help finding the rule, use filters in the **Filters/Tagging** pane (see Filter rules).

3. Select **New**, then click **Firewall Exception**.
4. Click **Add**, then select or type the values that define this exception.
5. Click **OK**.

**Deep packet inspection rules**

Deep packet inspection rules evaluate the contents of a packet and compare them with patterns in the rule signatures. When there is a match, the specified action is taken. The BASE filter (in the **Filters/Tagging** pane) provides protection against known intrusions that might be damaging to a system or its data. The same is true for the MALWARE and VIRUS filters. POLICY and MULTIMEDIA filters inhibit or alert on network activities associated with user-defined network usage specifications and are not associated with potentially dangerous network intrusions. These are the general filter group types:

- **Protective rules** (BASE, MALWARE, PERIMETER, VIRUS)
- **Policy rules** (CHAT, MULTIMEDIA, PEERTOPEER, POLICY, SECURE APPLICATION GATEWAY)

Typically, the default rules are sufficient for protecting the network. However, there might be an occasion where rules specific to a protected system or environment are required. You can add custom deep packet inspection rules to the ESM (see Add Deep Packet Inspection rules).


**Add deep packet inspection rules**

Add a custom deep packet inspection rule when one is needed for a protected system or environment.

**Task**

For option definitions, click ? in the interface.

1. On the Policy Editor, select Nitro IPS | Deep Packet Inspection.
2. Click New, then select Deep Packet Inspection Rule.
3. Define the settings, then click OK.

The filters in the new rule are applied and the new rule appears in the rule display pane. If you click the filter icon, the filtering is cleared and all the deep packet inspection rules are displayed.

**Add deep packet inspection attribute**

When you add or edit a deep packet inspection rule, one of the necessary steps is assigning attributes to the rule. These attributes define the action for the rule. You can add and delete custom options to the existing list so that they can be assigned to a rule.

**Task**

For option definitions, click ? in the interface.

1. On the Policy Editor, select IPS | Deep Packet Inspection | Add.
2. From the drop-down list, select the category for this attribute.
3. In the Options field, select the action associated with this attribute.
4. Enter a value for the option selected, then click OK.

The option name and value are added to the Rule options table. Select the value to edit or delete it.

**Internal rules**

The Internal rule type contains rules with signature IDs between 3,000,000 and 3,999,999, which are internal alerts and do not have signatures like other rules do. These rules can only be enabled or disabled.

This rule type is available only when a Nitro IPS or virtual device is selected in the system navigation tree.

**Manage internal rules**

View the list of existing internal rules or change their status.

**Task**

For option definitions, click ? in the interface.

1. On the system navigation tree, select a Nitro IPS or virtual device.
2. In the Rule Types pane of the Policy Editor, select IPS | Internal.
3. In the Enable column, click Select All, Select None, or select or deselect individual rules.
Filter rules
Filter rules allow you to specify the action to take when data that you define is received by the Receiver.

Data order
Filter rules are written to the Receiver in this data order:

1. All non "catch-all" rules.
   a. stop = true and parse = false and log = false
   b. stop = true and parse = true and log = true
   c. stop = true and parse = true and log = false
   d. stop = true and parse = false and log = true

2. All "catch-all" rules

Rule order
If you have Policy Administrator rights, you can define the order that you want the Filter rules to run in. These rules then run in the most effective order to generate the data you need (see Set order for ASP and Filter rules).

Add Filter rules
You can add Filter rules to the Policy Editor.

Task
For option definitions, click ? in the interface.

1. On the Policy Editor, select Receiver | Filter.
2. Select New, then click Filter Rule.
3. Complete the fields, then click OK
4. To enable the rule, select the rule in the rule display pane, click the setting in the Action column, then click enabled.

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

It is also ideal for sorting through complex log sources such as Linux and UNIX servers. This functionality requires you to write rules tailored to your Linux or UNIX environment.

Knowledge of regular expressions is needed to use this feature.

When the system receives an ASP log, the time format has to match the format specified in the ASP rule. If it doesn't, the log isn't processed. You can add multiple custom time formats to increase the likelihood that the time format for the log matches (see Add time format to ASP rules).

If you have Policy Administrator rights, you can define the order for running the ASP rules. These rules then generate the data you need (see Set order for ASP and Filter rules).
Add a custom ASP rule

The Advanced Syslog Parser Rule editor allows you to create rules to parse ASP log data.

Task
For option definitions, click ? in the interface.

1. On the Policy Editor, select Receiver | Advanced Syslog Parser.
2. Select New, then click Advanced Syslog Parser Rule.
3. Click each tab and fill in the information requested.
4. Click Finish.

Set order for ASP and Filter rules

If you have Policy Administrator rights, you can now set the execution order for Filter or ASP rules. This option sorts your rules efficiently to give you the data that you need most.

Task
For option definitions, click ? in the interface.

1. On the ESM console, click the Policy Editor icon.
2. On the Operations menu, select Order ASP Rules or Order Filter Rules, then select a data source in the Data source type field.
   The left pane is populated with the rules that are available to put in order. The ordered rules are in the right pane.
3. On the Standard Rules or Custom Rules tab, move a rule from the left pane to the right pane (drag and drop or use the arrows), placing them above or below Unordered Rules.
   Unordered Rules represents the rules in the left pane, which are those that are in default order.
4. Use the arrows to reorder the rules, then click OK to save the changes.

Add time formats to ASP rules

When the system receives an Advanced Syslog Parser (ASP) log, the time format has to match the format specified in the ASP rule.
You can add multiple custom time formats to increases the likelihood that the time format for the log will match one of the given formats.

Task
For option definitions, click ? in the interface.

1. On the ESM console, click the Policy Editor icon.
2. In the Rule Types pane, click Receiver | Advanced Syslog Parser.
3. After the ASP rules download, do one of the following:
   - To edit an existing rule, click the rule, then click Edit | Modify.
   - To add a new rule, click New | Advanced Syslog Parser Rule, then complete the General, Parsing, and Field Assignment tabs.
4. Click the Mapping tab, then click the plus icon above the Time Format table.
5 Click in the Format field, then select the time format.

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

- First Time and Last Time refer to the first and last time the event is generated. Any Custom Type time fields that you added to the ESM (see Custom type filters) are also listed.

7 Click OK, then complete the remaining information on the Mapping tab.

**Data source rules**

The list of data source rules includes predefined and auto learned rules.

The Receiver auto learns data source rules as it processes the information sent to it by the data sources that are associated with the Receiver.

The Data Source option in the Rule Types pane is only visible when a policy, data source, Advanced Syslog Parser, or Receiver is selected in the system navigation tree. The description area at the bottom of the page gives detailed information concerning the selected rule. All rules have a severity setting that dictates the priority associated with a rule. The priority impacts how the alerts generated for these rules are shown for reporting purposes.

Data source rules have a defined default action. The Receiver assigns it to the event subtype associated with the rule. You can change this action (see Set data source rule actions).

**Set data source rule actions**

Data source rules have a defined default action. The Receiver assigns this action to the event subtype associated with the rule. You can change this action.

You can set the value of the event subtype per data source rule. This means that you can set rule actions for dashboards, reports, parsing rules, or alarms with different values, such as the outcome of a selective access rule (permit/deny).

**Task**

For option definitions, click ? in the interface.

1 On the ESM console, click the Policy Editor icon, then select Receiver | Data Source in the Rule Types pane.

2 Click in the Subtype column for the rule you want to change, then select the new action.
   - Select enable to populate the event subtype with the default action, alert.
   - Select disable, if you don't want to collect events for the corresponding rule.
   - Select any other action to populate the event subtype with that action.

**Manage auto-learned data source rules**

View a list of all auto-learned data source rules and edit or delete them.

**Task**

For option definitions, click ? in the interface.

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.
On the **Origin** drop-down list, select **user defined**, then click the **Run Query** icon.

All the auto-learned data source rules are listed in the display pane.

Select the rule you want to edit or delete, click **Edit**, then select **Modify** or **Delete Auto Learned Rules**.
- If you selected **Modify**, change the name, description, or normalized ID, then click **OK**.
- If you selected **Delete Auto Learned Rules**, select the correct option, then click **OK**.

**Windows events rules**
Windows events rules are used to generate events that are Windows related.
They are data source rules for Windows events and are separated from the data source rule type because they are a common use case. All rules of this type are defined by McAfee. You can't add, modify, or delete them, but you can change their property settings.

**ADM rules**
McAfee ADM is a series of network appliances powered by the ICE Deep Packet Inspection (DPI) Engine.
The ICE Engine is a software library and collection of protocol and content plug-in modules that can identify and extract content from raw network traffic in real time. It can fully reassemble and decode application level content, transforming cryptic network packet streams into easily readable content as if it were being read from a local file.
The ICE engine is capable of automatically identifying protocols and content types without the need to rely on fixed TCP port numbers or file extensions. ICE engine does not rely on signatures to perform its analysis and decoding, instead its modules implement full parsers for each protocol or content type. This results in extremely accurate identification and decoding of content and allows content to be identified and extracted even when that content is compressed or otherwise encoded and, therefore, doesn't pass over the network in clear text.
As a result of this highly accurate identification and decoding, the ICE engine is able to offer a uniquely deep view of network traffic. For example, the ICE engine could receive a PDF document stream that traversed the network inside a .zip file, as a BASE-64 encoded attachment to an SMTP email from a SOCKS proxy server.
This application and document-awareness allow the ADM to provide invaluable security context. It can detect threats that can't be easily detected by a traditional IDS or Nitro IPS, such as:
- Leak of sensitive information and documents or communication policy violations.
- Unauthorized application traffic (for example, who's using Gnutella?).
- Applications being used in unexpected ways (for example, HTTPS on non-standard port).
- Potentially malicious documents (for example, document does not match its extension).
- New generation of exploits (for example, PDF document with an embedded executable).
The ADM also detects malicious traffic patterns by detecting anomalies in application and transport protocols (for example, an RPC connection is malformed or TCP destination port is 0).
**Supported applications and protocols**

There are more than 500 supported applications and protocols in which ADM can monitor, decode, and detect anomalies. Here is a sample list:

- Low-level network protocols — TCP/IP, UDP, RTP, RPC, SOCKS, DNS, and others
- Email — MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- Chat — MSN, AIM/Oscar, Yahoo, Jabber, IRC
- Webmail — AOL Webmail, Hotmail, Yahoo! Mail, Gmail, Facebook, and MySpace email
- P2P — Gnutella, bitTorrent
- Shell — SSH (detection only), Telnet
- Instant messaging — AOL, ICQ, Jabber, MSN, SIP, and Yahoo
- File transfer protocols — FTP, HTTP, SMB, and SSL
- Compression and extraction protocols — BASE64, GZIP, MIME, TAR, ZIP, and others
- Archive files — RAR Archives, ZIP, BZIP, GZIP, Binhex, and UU-encoded archives
- Installation packages — Linux packages, InstallShield cabinets, Microsoft cabinets
- Image files — GIFs, JPEGs, PNGs, TIFFs, AutoCAD, Photoshop, Bitmaps, Visio, Digital RAW, and Windows icons
- Audio files — WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast, and more
- Video files — AVI, Flash, QuickTime, Real Media, MPEG-4, Vivo, Digital Video (DV), Motion JPEG, and more
- Other applications and files — Databases, spreadsheets, faxes, web applications, fonts, executable files, Microsoft Office applications, games, and even software development tools
- Other protocols — Network printer, shell access, VoIP, and peer-to-peer

**Key concepts**

Key to understanding how ADM works is an awareness of the following concepts:

- **Object** — An object is an individual item of content. An email is an object but also an object container since it has a message body (or two) and attachments. An HTML page is an object which may contain additional objects such as images. A .zip file and each file within the .zip file are all objects. ADM unpacks the container and treats each object inside as its own object.

- **Transaction** — A transaction is a wrapper around the transfer of an object (content). A transaction contains at least one object; however, if that object is a container, like a .zip file, then the single transaction might contain several objects.

- **Flow** — A flow is the TCP or UDP network connection. A flow might contain many transactions.
**DEM rules**

The true power of McAfee DEM lies in the way it captures and normalizes the information in network packets.

DEM also has the ability to create complex rules using logical and regular expressions for pattern matching, which provides the ability to monitor database or application messages with virtually no false positives. The normalized data (metrics) vary for each application because some application protocols and messages are richer than others. Filter expressions must be carefully crafted, not only the syntax but also by making sure that the metric is supported for the application.

The DEM ships with a default set of rules. Default compliance rules monitor significant database events such as logon/logoff, DBA-type activity such as DDL changes, suspicious activity, and database attacks that are typically required to achieve compliance requirements. You can enable or disable each default rule and set the value of each rule’s user-definable parameters.

These are the types of DEM rules: Database, data access, discovery, and transaction tracking.

<table>
<thead>
<tr>
<th>Rule types</th>
<th>Description</th>
</tr>
</thead>
</table>
| Database   | The DEM default rule set includes rules for each supported database type and common regulations like SOX, PCI, HIPAA, and FISMA. You can enable or disable each of the default rules and set the value of each rule’s user-definable parameters.  
In addition to using the rules that are shipped with the DEM, you can create complex rules using logical and regular expressions. This provides the ability to monitor database or application messages with virtually no false positives. Because some application protocols and messages are richer than others, the normalized data (metrics) vary for each application.  
Rules can be as complex as you require and include both Logical and Regular Expression operators. A Rule Expression can be applied against one or more metrics available for the application. |
| Data access| The DEM’s data access rules provide the ability to track unknown access paths into the database and send alerts in real time. Common violations in database environments, such as application developers accessing production systems using application logon IDs, can be easily tracked once you create the appropriate data access rules. |
## Rule types

<table>
<thead>
<tr>
<th>Rule types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>The DEM’s database discovery rules provides an exception list of database servers, of the types supported by the ESM, that are on the network but are not being monitored. This allows a security administrator to discover new database servers being added to the environment and illegal listener ports opened to access data from databases. The discovery rules (Policy Editor</td>
</tr>
<tr>
<td>Transaction tracking</td>
<td>Transaction tracking rules allow you to track database transactions and auto-reconcile changes. For example, the time-consuming process of tracking database changes and reconciling them with authorized work orders in your existing change ticketing system can be fully automated. Use of this feature is best understood with an example: The DBA, as a matter of procedure, would execute the start tag stored procedure (spChangeControlStart in this example) in the database where the work would be performed before actually beginning the authorized work. The Transaction Tracking feature in the DEM allows the DBA to include up to three optional string parameters as argument to the tag in the correct sequence:  1 ID  2 Name or DBA Initials  3 Comment  For example, spChangeControlStart '12345', 'mshakir', 'reindexing app'  When the DEM observes the spChangeControlStart procedure being executed, it not only logs the transaction but also the parameters (ID, Name, Comment) as special information.  Once the work is complete, the DBA executes the end tag stored procedure (spChangeControlEnd) and optionally includes one ID parameter, which must the same as the ID in the begin tag). When the DEM observes the end tag (and ID) it can associate all activity between the start tag (which has the same ID) and end tag as a special transaction. You can now report by transactions and search by ID, which in this work order reconciliation example could be the change control number.  You can also use transaction tracking to log start and end of a trade execution or even begin and commit statements to report by transactions instead of queries.</td>
</tr>
</tbody>
</table>

## 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
<th>Database Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Name</td>
<td>The name that identifies the database type to which the rule applies.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Begin Time</td>
<td>Start timestamp of the query.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Begin Time Skew</td>
<td>Captures the server clock time skews.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Name</td>
<td>Definition</td>
<td>Database Types</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Client IP</td>
<td>Client's IP address.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Client Name</td>
<td>Name of the client machine.</td>
<td>MSSQL, Oracle, DB2, Sybase, Informix, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Client PID</td>
<td>Process ID assigned by the operating system to the client process.</td>
<td>MSSQL, DB2, Sybase, MySQL</td>
</tr>
<tr>
<td>Client Port</td>
<td>Port number of the client socket connection.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Command Name</td>
<td>Name of the MySQL command.</td>
<td>MSSQL, Oracle, DB2, Sybase, Informix</td>
</tr>
<tr>
<td>Command Type</td>
<td>Type of MySQL command: DDL, DML, Show or Replication.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Data In</td>
<td>Total number of bytes in the inbound query packet.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Data Out</td>
<td>Total number of bytes in the outbound result packets.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Database Name</td>
<td>Name of the database being accessed.</td>
<td>MSSQL, DB2, Sybase, MySQL, Informix, PostgreSQL, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>End Time</td>
<td>End of the completion timestamp query.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Error Message</td>
<td>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.</td>
<td>DB2, Informix</td>
</tr>
<tr>
<td>Message Number</td>
<td>A unique message number assigned by the database server to each error.</td>
<td>MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache</td>
</tr>
<tr>
<td>Message Severity</td>
<td>Severity level number between 10 and 24, which indicates the type and severity of the problem.</td>
<td>MSSQL, Sybase, Informix</td>
</tr>
<tr>
<td>Message Text</td>
<td>Full text of the message.</td>
<td>MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache</td>
</tr>
<tr>
<td>Name</td>
<td>Definition</td>
<td>Database Types</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Time</td>
<td>Time taken to send the result set back to the client (response_time - server_response_time).</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>NT Client Name</td>
<td>Windows machine name from which the user logged in.</td>
<td>MSSQL</td>
</tr>
<tr>
<td>NT Domain Name</td>
<td>Windows domain name from which user logged in.</td>
<td>MSSQL</td>
</tr>
<tr>
<td>NT User Name</td>
<td>Windows user login name.</td>
<td>MSSQL</td>
</tr>
<tr>
<td>Object Name</td>
<td></td>
<td>OSS User Name: MySQL, Oracle, DB2, Sybase, Informix</td>
</tr>
<tr>
<td>OSS User Name</td>
<td>Oracle</td>
<td></td>
</tr>
<tr>
<td>Package Name</td>
<td>A package contains control structures used to execute SQL statements. Packages are produced during program preparation and created using the DB2 subcommand BIND PACKAGE.</td>
<td>DB2</td>
</tr>
<tr>
<td>Packets In</td>
<td>Number of packets comprising the query.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Packets Out</td>
<td>Number of packets comprising the return result set.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, InterSystems Cache</td>
</tr>
<tr>
<td>Password Length</td>
<td></td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, InterSystems Cache</td>
</tr>
<tr>
<td>Query Block Size</td>
<td>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.</td>
<td>DB2, Informix</td>
</tr>
<tr>
<td>Query Exit Status</td>
<td>Exit status of a query.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache</td>
</tr>
<tr>
<td>Query Number</td>
<td>A unique number assigned to each query by the AuditProbe monitoring agent starting with zero for the first query and incrementing by one.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Query Text</td>
<td>The actual SQL query sent by the client.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Query Type</td>
<td>An integer number assigned to different type of queries.</td>
<td>MSSQL, Oracle, Sybase</td>
</tr>
<tr>
<td>Real User Name</td>
<td>Client user login name.</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Definition</td>
<td>Database Types</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Response Content</td>
<td>End-to-end response time of the query (server_response_time + network_time).</td>
<td>MSSQL, Oracle, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache</td>
</tr>
<tr>
<td>Response Time</td>
<td>Number of rows in the return result set.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Security Flag</td>
<td>Security flag metric whose value is set to 1 (TRUSTED) or 2 (UNTRUSTED)</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td></td>
<td>when access policy file criteria specified by the administrator is met.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value of 3 indicates that policy file criteria were not met. Value of 0 indicates that security monitoring has not been turned on.</td>
<td></td>
</tr>
<tr>
<td>Security Mechanism</td>
<td>The security mechanism that is used to validate the user's identity</td>
<td>DB2</td>
</tr>
<tr>
<td></td>
<td>(for example, User ID and password).</td>
<td></td>
</tr>
<tr>
<td>Server IP</td>
<td>IP address of the database server host.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache</td>
</tr>
<tr>
<td>Server Name</td>
<td>This is the name of the server. The host name is assigned as the server name by default.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Server Port</td>
<td>Port number of the server.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, InterSystems Cache</td>
</tr>
<tr>
<td>Server Response Time</td>
<td>Initial response from the database server to the client query.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>Severity Code</td>
<td></td>
<td>DB2</td>
</tr>
<tr>
<td>SID</td>
<td>Oracle system identifier.</td>
<td>Oracle, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
<tr>
<td>SPID</td>
<td>Database system process ID assigned to each unique connection/session.</td>
<td>MSSQL, Sybase</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
<th>Database Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Code</td>
<td>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:</td>
<td></td>
</tr>
<tr>
<td>SQL Command</td>
<td>Type of SQL command.</td>
<td></td>
</tr>
<tr>
<td>SQL State</td>
<td>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.</td>
<td>DB2</td>
</tr>
<tr>
<td>User Name</td>
<td>Database user login name.</td>
<td>MSSQL, Oracle, DB2, Sybase, MySQL, Informix, PostgreSQL, Teradata, PIServer, InterSystems Cache</td>
</tr>
</tbody>
</table>

### Correlation rules

The fundamental purpose of the correlation engine is to analyze data flowing from ESM, detect interesting patterns within the data flow, generate alerts that represent these patterns, and insert these alerts into the Receiver's alert database. The correlation engine is enabled when a correlation data source is configured.

Within the correlation engine, an interesting pattern results in data interpreted by a correlation rule. A correlation rule is totally separate and distinct from a firewall or standard rule and has an attribute that specifies its behavior. Each receiver gets a set of correlation rules from an ESM (deployed correlation rule set), which is composed of zero or more correlation rules with any user-defined parameter values set. Like firewall and standard rule sets, a base correlation rule set will be included with every ESM (base correlation rule set), and updates to this rule set are deployed to ESM devices from the rule update server.

Only one correlation data source can be configured per Receiver, in a fashion similar to configuring syslog or OPSEC. Once the correlation data source is configured, you can edit the base correlation rule set to create the deployed correlation rule set using the **Correlation Rule Editor**. You are allowed to enable or disable each correlation rule and set the value of each rule's user definable parameters.

In addition to enabling or disabling the correlation rules, the **Correlation Rule Editor** allows you to create custom rules and create custom correlation components that can be added to correlation rules.

The rules on the rule update server include default values. When you update the base correlation engine rule set, you must customize these default values so they properly represent your network. If you deploy these rules without changing the default values, they can generate false positives or false negatives.

The fundamental purpose of the correlation engine is to analyze data flowing from ESM, detect interesting patterns within the data flow, generate alerts that represent these patterns, and insert these alerts into the Receiver's alert database. The correlation engine is enabled when a correlation data source is configured.
View correlation rule details

Correlation rules now display details about what caused the rule to trigger. This information can help you tune for false positives.

Details are always gathered at the time of request in the user interface. However, for rules that use dynamic watchlists or other values that might change often, you can set the rule to get details immediately after triggering. This reduces the chance that details are no longer available.

Task

For option definitions, click ? in the interface.

1. Set each rule to show the details immediately:
   a. On the ESM console, click the **Correlation** quick launch icon.
      The **Policy Editor** opens with the **Correlation** rule type selected.
   b. Click in the **Details** column for the rule and select **On**.
      You can select more than one rule at a time.

2. View the details:
   a. On the system navigation tree, click **Rule Correlation** under the ACE device.
   b. On 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.

Add custom ADM, database, or correlation rules

In addition to using the predefined ADM, Database, or Correlation rules, you can create complex rules using logical and regular expressions. The editors you use to add these different rule types are very similar to each other so they are described in the same sections.

Task

For option definitions, click ? in the interface.

1. In the **Rule Types** pane of the **Policy Editor**, select **ADM**, **DEM** | **Database**, or **Correlation**.
2. Click **New**, then select the rule type you are adding.
3. Enter the information requested, then drag-and-drop logical elements and expression components from the toolbar to the **Expression Logic** area to build the rule's logic.
4. Click **OK**.
Tasks

- **Add parameters to a correlation rule or component on page 307**
  The parameters of a correlation rule or component control the behavior of the rule or component when it executes. Parameters are not required.

- **Add or edit a data access rule on page 309**
  DEM data access policies provide the ability to track unknown access paths into the database and to send events in real-time.

- **Add or edit a transaction tracking rule on page 310**
  Transaction tracking rules track database transactions and auto-reconcile changes, as well as log start and end of a trade execution or begin and commit statements to report by transactions instead of queries.

- **Manage custom ADM, DEM, or correlation rules on page 310**
  Copy a predefined rule and use it as a template for a custom rule. When you add a custom rule, you can edit the settings, copy and paste it to use it as a template for a new custom rule, or delete it.

- **Set up rule and report for database audit trails on page 311**
  A Privileged User Audit Trails report allows you to view the audit trail for modifications made to the database or to track access to a database or table that was associated with a specific database event.

Logic elements

When you add an ADM, database, and correlation rule or correlation component, you must build the core functionality of the rule by dragging the logical elements to the **Expression Logic** or **Correlation Logic** area. The logical elements set the framework for the rule.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AND</td>
<td>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 the conditions under this logical element to be met before a rule is triggered.</td>
</tr>
<tr>
<td>OR</td>
<td>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.</td>
</tr>
<tr>
<td>SET</td>
<td>For correlation rules or components, this element allows you to define more than one condition and select the number of conditions that must be true for the rule to be triggered. For example, if you have three conditions in the set and two of them must be met before the rule is triggered, the set reads &quot;2 of 3.&quot;</td>
</tr>
</tbody>
</table>

Each of these elements has a menu with at least two of these options:

- **edit** — You can edit the default settings (see **Edit logic elements default settings**).

- **remove logical element** — You can delete the selected logical element. If it has any children, they aren't deleted and move up in the hierarchy.

  This doesn't apply to the root element (the first one in the hierarchy). If you remove the root element, all the children are also removed.

- **remove logical element and all of its children** — You can delete the selected element and all of 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.
**Edit logical elements**
The AND, OR, and SET logical elements have default settings. These can be changed on the Edit Logic Element page.

**Task**
For option definitions, click ? in the interface.

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.

**Add parameters to a correlation rule or component**
The parameters of a correlation rule or component control the behavior of the rule or component when it executes. Parameters are not required.

**Task**
For option definitions, click ? in the interface.

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.

**Example of custom correlation rule or component**
Add a correlation rule or component.

The rule we are going to add in this example generates an alert when the ESM detects five unsuccessful login attempts from a single source on a Windows system, followed by a successful login, all within 10 minutes.

1. In the Rule Types pane of the Policy Editor, click Correlation.
2. Click New, then select Correlation Rule.
3. Type a descriptive name, then select the severity setting.
   - Because an event generated by this rule could indicate that an unauthorized person has accessed the system, an appropriate severity setting is 80.
4 Select the normalization ID, which could be Authentication or Authentication | Login, then drag-and-drop the AND logic element.

Select AND because there are two types of actions that need to occur (login attempts first, then a successful login).

5 Click the Menu icon , then select Edit.

6 Select Sequence to indicate that the actions (first, five unsuccessful login attempts and second, a successful login) must occur sequentially, then set the number of times this sequence must occur, which is "1."

7 Set the period of time the actions need to occur in, then click OK.

Since there are two actions that require time windows, the 10-minute period must be divided between the two. For this example, five minutes is the period of time for each action. Once the unsuccessful attempts have occurred within five minutes, the system begins to listen for a successful login from the same IP source within the next five minutes.

8 In the Group by field, click the icon, move the Source IP option from the left to the right, indicating that all actions must come from the same source IP, then click OK.

9 Define the logic for this rule or component.
To do this... | Do this...
---|---
Specify the type of filter that identifies the events of interest (in this case, multiple failed login attempts against a Windows system). | 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 login failure needs to occur and the period of time 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 five separate attempts that must occur. The element allows you to set the number of times and the length of time that they must occur.  
2. Click the Menu icon for the AND element you just added, then click Edit.  
3. In the Threshold field, enter 5 and remove other values that are present.  
4. Set the Time Window field to 5.  
5. Click OK.

Define the second filter type that needs to occur, which is the successful login. | 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.

The new rule is added to the list of correlation rules on the Policy Editor.

**Add or edit a data access rule**

DEM data access policies provide the ability to track unknown access paths into the database and to send events in real-time. Common violations in database environments, such as application developers accessing production systems using application logon IDs, can be easily tracked when create the appropriate data access policies.
**Task**
For option definitions, click ? in the interface.

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

2. Do one of the following:
   - To add a new rule, select New, then click Data Access Rule
   - To edit a rule, select the rule in the rules display pane, then click Edit | Modify.

3. Fill in the information, then click OK.

**Add or edit a transaction tracking rule**
Transaction tracking rules track database transactions and auto-reconcile changes, as well as log start and end of a trade execution or begin and commit statements to report by transactions instead of queries.

**Task**
For option definitions, click ? in the interface.

1. On the Policy Editor, select DEM | Transaction Tracking.

2. Do one of the following:
   - To add a new rule, click New, then click Transaction Tracking Rule.
   - To edit a rule, select the rule on the rules display pane, then click Edit | Modify.

3. Fill in the information, then click OK.

**Manage custom ADM, DEM, or correlation rules**
Copy a predefined rule and use it as a template for a custom rule. When you add a custom rule, you can edit the settings, copy and paste it to use it as a template for a new custom rule, or delete it.

**Task**
For option definitions, click ? in the interface.

1. On the Policy Editor, select ADM or DEM | Database, Data Access, or Transaction Tracking.

2. Do any of the following:
### To... | Do this...
---|---
View all custom ADM or DEM rules | 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.  
The custom rules of the type you select are listed in the rule display pane.

Copy and paste a rule | 1. Select a predefined or custom rule.  
2. Click Edit | Copy.  
3. Click Edit | Paste.  
The rule you copied is added to the list of existing rules, with the same name.  
4. To change the name, click Edit | Modify.

Modify a custom rule | 1. Select the custom rule.  
2. Click Edit | Modify.

Delete a custom rule | 1. Select the custom rule.  
2. Click Edit | Delete.

### Set up rule and report for database audit trails

A Privileged User Audit Trails report allows you to view the audit trail for modifications made to the database or to track access to a database or table that was associated with a specific database event. After the parameters for generating this report are set up, you receive compliance report notifications that display the audit trail associated with each event. To generate the audit trail events, you must add a Data Access rule and a Privileged User Audit Trails report.

**Task**

For option definitions, click ? in the interface.

1. In the Rule Types pane of the Policy Editor, select DEM | Data Access.
2. Highlight DEM - Template Rule - Trusted Use Access From IP Range in the rules display pane.
3. Click Edit | Copy, then click Edit | Paste.
4. Change the name and properties of the new rule.  
   a. Highlight the new rule, then select Edit | Modify.  
   b. Enter a name for the rule, then type the user name.  
   c. Select the Untrusted action type, then click OK.
5. Click the Rollout icon 📦.
6. Set up the report:  
   a. On System Properties, click Reports | Add.  
   b. Fill in sections 1 – 3, and 6.
c  In section 4, select Report PDF or Report HTML.

d  In section 5, select Compliance | SOX | Privileged User Audit Trails (Database).

e  Click Save.

7  To generate the report, click Run Now.

ESM rules
ESM rules are used to generate events that are related to the ESM.
All the rules of this type are defined by McAfee. They can be used to generate compliance or auditing reports that show what has occurred on the ESM. You cannot add, modify, or delete them. You can, however, change the property settings (see Rule types and their properties).

Normalization
Rules are named and described by each vendor. As a result, the same type of rule often has different names, making it difficult to gather information for the types of events that are occurring.
McAfee compiled, and continually updates, a list of normalized IDs that describe rules so that events can be grouped into useful categories. When you click Normalization in the Rule Types pane of the Policy Editor, these IDs, names, and descriptions are listed.

These event features offer the option to organize event information using normalized IDs:

- View component fields — Normalized Event Summary is an option when defining fields for an event query in the pie chart, bar chart, and list components (see Manage a query).

- View component filters — When you are creating a new view, you can select to filter event data on a component by the normalized IDs (see Manage a query).

- View filters — Normalized ID is an option on the list of view filters (see Filtering views).

- View list — A Normalized Event Summary view is available on the list of Event Views.

The Details tab on the Event Analysis view lists the normalization ID for the events that appear on the list.

When you are adding Normalized ID filters to a new or existing view, you can:

- Filter by all the normalized IDs in a first-level folder. A mask (/5 for a first-level folder) is included at the end of the ID to indicate that the events will also be filtered by the child IDs of the selected folder.

- Filter by the IDs in a second- or third-level folder. A mask (/12 for a second-level folder, /18 for a third-level folder) is included at the end of the ID to indicate that the events are filtered by the child IDs of the selected subfolder. The fourth level doesn't have a mask.

- Filter by a single ID.

- Filter by multiple folders or IDs at one time using the Ctrl or Shift keys to select them.

Enable Copy Packet
When Copy Packet is enabled for a rule, the packet data is copied to the ESM. If enabled, packet data is included within the source event data of an Internal Event Match or Field Match alarm.
Task
For option definitions, click ? in the interface.

1. On the ESM console, click the Policy Editor icon.

2. In the Rule Types pane, click the type of rule that you want to access, then locate the rule in the rule display pane.

3. Click the current setting in the Copy Packet column, which is off by default, then click on.

Default Policy settings
You can set up the default policy to operate in alerts only mode or oversubscription mode. You can also view the status of the rule updates and initiate an update.

Alerts Only Mode
Policies can be applied to Nitro IPS and virtual devices in Alerts Only Mode.

When Alerts Only Mode is turned on, all enabled rules are sent to the devices with a usage of alerts, even if the rule is set to a blocking action such as Drop. When viewing the events generated, the Event Subtype column lists the action as Alert, followed by the action taken if it was not in Alerts Only Mode, such as Alert-Drop. This is useful for system administrators who are still becoming familiar with their network traffic patterns, allowing them to analyze events generated without actively blocking any events, but seeing the action that is taken when Alerts Only Mode is turned off.

Turning on Alerts Only Mode doesn't change individual usage settings for individual rules in the Policy Editor. For example, when it is on, a rule might be sent to the Nitro IPS or virtual device with a usage of alerts even though its usage in the Policy Editor is set to Drop (with the exception of a rule set to Pass, which remains in that mode). This allows you to easily turn Alerts Only Mode on and off without otherwise affecting your policy settings. Alerts Only Mode does not affect disabled rules. Rules are never sent to a device when set to Disable.

Enable Alerts only mode
If you want all enabled rules sent to the devices with a usage of alerts, you must turn on the Alerts only mode feature. Inheritance applies to this setting so this policy's setting overrides the value it would otherwise inherit.

Task
For option definitions, click ? in the interface.

1. On the Policy Editor, click the Settings icon.

2. In the Alerts only mode field, select On.

Set up Oversubscription Mode
Oversubscription Mode defines how packets are handled if the device's capacity is exceeded. In each case, the packet is recorded as an event.
Task
For option definitions, click ? in the interface.

1 On the Policy Editor, click the Settings icon.

2 In the Oversubscription Mode field, click Update.

3 In the Value field, enter the functionality.
   a Pass (pass or 1) allows packets that would be discarded to pass unscanned.
   b Drop (drop or 0) drops packets that exceed the device's capacity.
   c To pass or drop a packet without generating an event, enter spass or sdrop.

4 Click OK.

As of version 8.1.0, changing Oversubscription Mode affects the device and its children (virtual devices).
For this change to take effect, you must change the mode on the parent device.

View policy update status for devices
View a summary of the status of policy updates for all devices on the ESM.
This helps determine when you must roll out updates to your system.

Task
For option definitions, click ? in the interface.

1 On the Policy Editor, click the Settings icon.

2 In the Status field, view the number of devices that are up to date, out of date, and scheduled for an auto rollout.

3 Click Close.

Rule operations
There are several operations you can perform on the rules to manage them and generate the information needed.

Manage rules
ADM, DEM, Deep Packet Inspection, Advanced Syslog Parser, and Correlation rules can be viewed, copied, and pasted. Custom rules of these types can be modified or deleted. Standard rules can be modified, but must be saved as a new custom rule.

Task
For option definitions, click ? in the interface.

1 In the Rule Types pane of the Policy Editor, select the type of rule that you want to work with.

2 Do any of the following:
To do this... | Do this...  
---|---  
View custom rules | 1 Select the Filter tab in the Filters/Tagging pane.  
2 At the bottom of the pane, click the Advanced bar.  
3 In the Origin field, select user defined, then click Run Query.  

Copy and paste a rule | 1 Select a predefined or custom rule.  
2 Select Edit | Copy, then select Edit | Paste.  
The rule you copied is added to the list of existing rules, with the same name.  
3 To change the name, select Edit | Modify.  

Modify a rule | 1 Highlight the rule you want to view, then select Edit | Modify.  
2 Change the settings, then click OK. If it's a custom rule, it's saved with the changes. If it is a standard rule, you are prompted to save the changes as a new custom rule. Click Yes.  
If you did not change the name of the rule, it is saved with the same name and a different sigID. You can change the name by selecting the rule, then selecting Edit | Modify.  

Delete a custom rule | • Select the custom rule.  
  • Select Edit | Delete.  

Import rules  
You can import a set of rules that has been exported from another ESM and save it to your ESM.  

Task  
For option definitions, click ? in the interface.  

1 In the Rule Types pane of the Policy Editor, click the type of policy or rules you are importing.  
2 Click File | Import, then select Rules.  
   These changes are not tracked so they can't be undone.  
3 Click Import Rules, then browse to the file you want to import and select Upload.  
The file is uploaded to the ESM.  
4 On the Import Rules page, select the action to take if rules being imported have the same ID as existing rules.  
5 Click OK to import the rules, resolving the conflicts as indicated.  
The contents of the file are reviewed and the appropriate options are enabled or disabled, depending on the contents of the selected file.
Conflicts when importing correlation rules

When you export correlation rules, a file is created that contains the rule data. It doesn’t, however, include referenced items such as variables, zones, watchlists, custom types, and assets, which this rule might use.

When the export file is imported to another ESM, any referenced items contained in the rule that do not exist on the importing system results in a rule conflict. For example, if rule one references variable $abc, and no variable is defined on the importing system that is named $abc, this condition is a conflict. Conflicts are logged and the rule is flagged as in conflict.

Conflicts are resolved by creating the needed referenced items (manually or through import where applicable) or editing the correlation rule and changing the references within the rule.

If there are rules in conflict, a page is displayed immediately after the import process indicating which rules are in conflict or which failed. Rules can be edited to resolve conflicts from that page, or the page can be closed. Rules in conflict are flagged with an exclamation mark icon indicating their status. Editing a conflicted rule in the rule editor presents a conflicts button, which when clicked, displays the conflict detail for that rule.

Import variables

You can import a file of variables and change their type. If there are conflicts, the new variable is automatically renamed.

Before you begin
Set up the file to be imported.

Task
For option definitions, click in the interface.

1. In the Rule Types pane of the Policy Editor, click Variable.
2. Click File | Import | Variables, then browse to the file of variables and click Upload.
   - If there are conflicts or errors in the file, the Import - Error Log page opens informing you of each issue.
3. On the Import Variable(s) page, click Edit to change the Type for the selected variables.
4. Click OK.

Export rules

Export custom rules or all the rules in a policy and then import them to another ESM.

Task
For option definitions, click in the interface.

1. In the Rule Types pane of the Policy Editor, click the type of rules you are exporting.
2. Access a list of the custom rules of the type you selected:
   a. In the Filter/Tagging pane, make sure the Filter tab is selected.
   b. Click the Advanced bar at the bottom of the pane.
c On the Origin drop-down list, select user defined.
d Click the Run Query icon.

3 Select the rules you want to export, then click File | Export | Rules.
4 On the Export Rules page, select the format to use when exporting the rules.
5 On the Download page, click Yes, select the location, then click Save.

If you open the csv file using Microsoft Excel, some of the UTF-8 characters might be corrupted. To correct this, open the Text Import Wizard in Excel and select Delimited and Comma.

Set rules to auto-blacklist
You can mark rules to auto-blacklist. The IP address or IP address and port of the offender is added to the blacklist when the conditions you define are met.

Task
For option definitions, click ? in the interface.

1 In the Rule Types pane of the Policy Editor, expand IPS, then select the type of rule. For example, to set virus rules to auto-blacklist, select Deep Packet Inspection.
2 On the Filters tab in the Filters/Tagging pane, select the filter. Using the previous example, select Virus.
3 Click the Refresh icon.

The filtered rules are listed in the rules display area.
4 Click the header in the Blacklist column or select rules on the list, then click IP or IP & port.
5 Roll out the changes by clicking the Rollout icon in the upper-right corner, then close the Policy Editor.
6 Select a Nitro IPS or virtual device on the system navigation tree, then click the Properties icon.
7 Click Blacklist, then click Settings.
8 On the Auto-Blacklist Settings page, define the settings, then click OK.

Filter existing rules
When you select a rule type in the Policy Editor, all the rules of the selected type are listed in alphabetical order, by default. You can list them by time or use tags to filter the rules so you can view only those that meet your criteria.

Task
For option definitions, click ? in the interface.

1 In the Rule Types pane of the Policy Editor, select the type of rule you want to filter.
2 Make sure that the Filter tab is selected in the Filters/Tagging pane.
3 Do any of the following:
<table>
<thead>
<tr>
<th><strong>To...</strong></th>
<th><strong>Do this...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter with multiple tags</td>
<td>• Select categories or tags, then click the Run Query icon 🔎. Only those rules that meet all filters are displayed.</td>
</tr>
</tbody>
</table>
| View rules that meet either of the filters you select | 1 Select more than one category or tag.  
2 Click the or icon, then click the Run Query icon.  

*Fields that are affected by inheritance (Action, Severity, Blacklist, Aggregation, and Copy Packet) cannot be filtered using the or icon.*  

| Search for a specific tag                      | 1 Type the tag’s name in the Type here to search for a tag field.  
2 Select the one you need from the list of options.                                                                                                                        |
| List the rules by the time they were created   | • Click the Sort on Time icon 🕒 on the toolbar, then click the Run Query icon.                                                                                                                                                     |
| List the rules in alphabetical order           | • Click the Sort on Name icon 🕒 on the toolbar, then click the Run Query icon.                                                                                                                                                     |
| Clear the filtering                            | • Click the orange filter icon on the rules display pane title bar 📃. The filters are cleared and all the rules are once again displayed in the rule display pane.                                                                 |
| Clear the filter tags                          | • Click the Clear All icon 🖐️ on the toolbar.  
The tags are cleared but the list of rules remains filtered.                                                                                                                |
| Filter by signature ID                         | 1 Click the Advanced bar at the bottom of the Filter pane.  
2 Type the signature ID, then click the Run Query icon.                                                                                                                  |
| Filter by name or description                  | 1 In the Advanced pane, enter the name or description.  
2 For the results, regardless of case, click the case-insensitive icon Aa.                                                                                                                                                       |
| Filter by device type, normalized ID, or action| 1 In the Advanced pane, click the Filter icon 📃.  
2 On the Filter Variables page, select the variable.                                                                                                                       |
| Compare the differences in the policy-based settings for a rule type and its immediate parent | • In the Advanced pane, select View Exceptions, then click the Run Query icon.                                                                                                                                                     |
| Filter by severity, blacklist, aggregation, copy packet, origin, and rule status | • Select the filter from the drop-down list in each of these fields.                                                                                                                                                                 |
| View only custom rules                         | • Select user-defined in the Origin field in the Advanced pane, then click the Run Query icon.                                                                                                                                       |
| View rules created in a specific time period   | 1 Click the calendar icon next to the Time field on the Advanced pane.  
2 On the Custom Time page, select the start and stop time, click OK, then click the Run Query icon.                                                                          |
View a rule's signature
If you access the McAfee online signature database, you can view information about the signature for a rule. This option is available for firewall, deep packet inspection, and data source rules.

Task
For option definitions, click ? in the interface.

1 In the Rule Types pane of the Policy Editor, select the type of rule you want to view.
2 Select a rule in the rule display pane.
3 Click Operations, then select Browse Reference.
   The NTAC Vulnerability Summary screen opens in your browser.
4 To view the summary of a signature, click on the links in the Signatures section of the screen.

Retrieve rule updates
The rule signatures used by a Nitro IPS or virtual device to examine network traffic are continuously updated by the McAfee Signature Team and are available for download from the central server. These rule updates can be retrieved automatically or manually.

Task
See Override action on downloaded rules to set up overrides for the actions taken when rules are retrieved from the server.

For option definitions, click ? in the interface.

1 On the Policy Editor, click the Settings icon.
2 On the Rules Update line, click Update.
3 Set the ESM to retrieve the updates automatically or check for updates now.
4 If updates were downloaded manually, click the Rollout icon to apply them.
5 To view the manual updates, do the following:
   a In the Filters/Tagging pane, click the Advanced bar.
   b In the Rule Status field, selected Updated, New, or Update/New to indicate the type of updated rules you want to view.
   c Click the Run Query icon.

The updated rules are listed with a starburst icon if they are added or an exclamation mark if they are modified.

Clear updated rule status
When rules are modified or added to the system. You can clear these markings once you have had the opportunity to review the updates.
**Task**
For option definitions, click ? in the interface.

1. In the **Rule Types** pane of the **Policy Editor**, select the type of rule you want to clear.

2. Do one of the following:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Clear all the rule status markings | 1. Click **Operations**, then select **Clear Updated Rule Status**.  
2. Click **All**. |
| Clear selected rules | 1. In the **Filters/Tagging** pane, click the **Advanced** bar.  
2. In the **Rule Status** field, select **Updated**, **New**, or **Updated/New** to indicate the type of marking you want to clear.  
3. Click the **Run Query** icon .  
The rules with the selected markings are listed in the rule display pane.  
4. Select the rules to be cleared.  
5. Click **Operation | Clear Updated Rule Status | Selected**. |

**Compare rule files**
You can compare the policy state (applied, current, rollback, or staged) of Nitro IPS, Receiver, ADM, and DEM rule files.

This is helpful if you need to see what would change if you apply the current policy to a device. In that case, you would compare the current rules and the applied rules.

**Task**
For option definitions, click ? in the interface.

1. On the system navigation tree, click a Nitro IPS, Receiver, ADM, or DEM device.

2. Click the **Policy Editor** icon in the actions toolbar, then click **Tools | Compare Rule Files**.

3. Make the selections, view the results, then click **Close**.

**View the rule change history**
You can view the rules that were changed, updated, or added to the system, as well as the latest version of each rule.

**Task**
For option definitions, click ? in the interface.

1. On the **Policy Editor**, click **Tools | Rule Change History**.

2. On the **Rule History** page, view the changes made to rules, or click the **Rule Version** tab to see the latest version of each rule.

3. Click **Close**.
Create a new watchlist of rules
A watchlist is a grouping of specific types of information that can be used as filters or as an alarm condition so you are notified when they occur in an event. These watchlists can be global or specific to an ESM user or group.

Task
For option definitions, click ? in the interface.

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

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

The Add Watchlist page lists the rules you selected.

3 Type a name, then make sure the Static radio button is selected.

i See Add a new watchlist to add a dynamic watchlist.

4 Select the type of data this watchlist is watching for, then select the assignee.

A user with administrator privileges can assign a watchlist to anyone or any group on the system. If you do not have administrator privileges, you can only assign watchlists to yourself and groups you are a member of.

5 To add more values to the watchlist, you can do so in the following ways:
   • To import a file of values in new-line-separated values format, click Import, then select the file.
   • To add individual values, type one value per line in the Values box.

i Maximum number of values is 1000.

6 To receive an alarm when an event is generated that contains any of the values on this watchlist, click Create Alarm.

7 Click OK.

Add rules to a watchlist
After creating a watchlist, you might need to add rule values to it. The Append to watchlist option provides a way for you to do that.

Task
For option definitions, click ? in the interface.

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.
Assign tags to rules or assets

You can assign tags to rules, indicating their attributes, and then filter the rules by their tags. The ESM has a predefined set of tags but also provides you with the ability to add new tags and new tag categories.

The Tags tab is not available for Variable, Preprocessor, or Normalization rule types.

Task

For option definitions, click ? in the interface.

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:

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Add a new tag category | 1. Click the New Category Tag icon 🎯.  
2. Type the name for the category.  
3. If you want this tag to be used in event severity calculation, select Use tag for event severity calculation, then click OK. |
|                      | The category is added with a base tag. You can add new tags under this category. |
| Add a new tag         | 1. Click the category you want to add the tag to, then click the New Tag icon 🎯.  
2. Type the name for the tag.  
3. If you want this tag to be used in event severity calculation, select Use tag for event severity calculation, then click OK. |
| Edit an existing category or tag | 1. Click the category or tag you want to edit, then click the Edit Tag icon 🎯.  
2. Change the name or setting, then click OK. |
| Delete a custom tag   | 1. Highlight the tag you want to delete, then click the Remove Tag icon ✗.  
2. Click Yes to confirm. |

Modify aggregation settings

Aggregated events are events that have fields that match.

Aggregation is selected by default and you can choose the type of aggregation to be used for all events generated on a device on the Event Aggregation page for each device. You can modify the aggregation settings for individual rules.

Task

For option definitions, click ? in the interface.

1. In the Rule Types pane of the Policy Editor, select the type of rule.
2. Select the rule for which you want to modify aggregation settings.
3 Click Operations on the toolbar and select Modify Aggregation Settings.

4 Select the field types you want to aggregate from the Field 2 and Field 3 drop-down lists.

   ! The fields you select must be different types or an error results.

5 Click OK to save the settings.

6 If you made changes that affect the way devices aggregate, you are asked if you want to roll out the changes. Do the following:
   a Click Yes.
      
      The Aggregation Exceptions Rollout page shows the status of the devices affected by this change. All devices that are out of date are checked.
   b If needed, deselect the checkmark from the devices you do not want to apply the changes to.
   c Click OK to roll out the changes.

      The Status column reflects the status of the update as the changes are rolled out.

---

Override action on downloaded rules

When rules are downloaded from the central server at McAfee, they have a default action assigned to them.

You can define an override action for rules of the type that you select when they are downloaded. If there is no override action defined, the rules take their default action.

**Task**

For option definitions, click ? in the interface.

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.

---

Severity weights

Event severity is calculated based on the severity weight given to assets, tags, rules, and vulnerabilities.

Each of the four severities is weighted in the final calculation. This final calculation is the sum of each of the four severities multiplied by their respective weights. The Severity Weights page shows the weights that are associated with the assets, tags, rules, and vulnerability groups. The sum of the settings must equal 100. When you change one setting, some or all other settings are affected. Here is a description of each type of severity:
### Severity type Descriptions

<table>
<thead>
<tr>
<th>Severity type</th>
<th>Descriptions</th>
</tr>
</thead>
</table>
| Asset         | An asset is an IP address, optionally within a zone. The asset severity of an event is determined as follows:  
   1. The destination IP address and destination zone of the event are compared against all assets. If a match is found, the severity of that asset is used as the asset severity for this event.  
   2. If no destination IP address and destination zone match is found, the source IP address and source zone of the event are compared against all assets. If a source IP address and source zone match is found, the severity of the asset is used as the asset severity for this event.  
   3. If no matches are found, the asset severity is zero. |
| Tag           | The tag severity is calculated using both McAfee and user-defined tags. For a tag to be used in the severity calculation, it must be set for both the rule and asset of the event. If the rule or asset does not have any tags defined or if there were no asset matches, the tag severity is zero. To calculate the tag severity, the number of matching rule and asset tags is multiplied by 10. The tag severity is limited to 100. |
| Rule          | The rule severity is the severity set for the event when it was created. It is based on the event's rule severity, as set in the Policy Editor, and any data enrichment configured for the event's collector. |
| Vulnerability | If VA SVE information is available for an event's asset and rule, then the highest severity of all matching asset and rule VA SVEs is used for the vulnerability severity, otherwise zero it used. |

### Set the severity weights

Asset, tag, rule, and vulnerability severities are weighted when calculating event severity. You must define these severities.

**Task**
For option definitions, click ? in the interface.

1. On the Policy Editor, click the Severity Weights icon.
2. Define the settings, then click OK.

### View policy change history

You can view or export a log of the changes that have been made to the policy. This log can hold a maximum of 1GB of data. When it reaches this limit, the oldest files are deleted as needed.

**Task**
For option definitions, click ? in the interface.

1. On the Policy Editor, click the View Policy Change History icon.
2. View or export a log, then click Close.
Apply policy changes

When you make changes to policies, you must roll out the changes to apply them. Changes made at the default policy level are applied to all policies when you roll out to all devices.

**Task**
For option definitions, click ? in the interface.

1. On the Policy Editor, click the Rollout icon.
2. Select how you want the rollout to occur.
3. Click OK.

After each device completes the rollout, the status of the policy will indicate a successful rollout. If the rollout command was unsuccessful, a page shows a summary of the failed commands.

Manage priority traffic

You can set up traffic to pass through the Nitro IPS without being tested against any rules. For example, it might be necessary to set up Voice over Internet Protocol (VoIP) traffic to cross over the Nitro IPS without taking time to check.

**Task**
For option definitions, click ? in the interface.

1. On the Policy Editor, click the Variable rule type.
2. Expand the priority_traffic category, then click PRIORITY_TRAFFIC_LIST.
3. Click Edit, then select Modify.
4. Manage the settings, then click OK.
Managing policies and rules

Manage priority traffic
alarms (continued)
  copy 213
  create 200
  create new from view event 248
  customize summary 214
  delete 215
  disable 213
  enable 213
  log 199
  manage recipients 215
  notifications 154
  notifications, add recipients 154
  pane 26
  pane, show 27, 173
  power failure notification 164, 205
  report files, manage 216
  reports, view and manage 216
  set up and manage 199
  severity symbols 199
  templates, add 214
  templates, manage 214
  Threat Intelligence Exchange alarms 144
  view details 215
alerts only mode
  enable 313
  policies 313
allocation, define data limits 171
Altiris server, retrieve data 277
analysis report, generate IPS 148
anomaly detection
  variables, edit 148
  wizard 147
apply configuration settings to DEM 136
archive
  set up inactive partitions 170
  settings, define for Receiver 63
ArcSight, add data source 96
ASN
  define settings for device 42, 221
  lookup from view 248
  lookup, perform 249
ASP rules
  set order 295
  time formats, add 295
asset manager 280
asset sources 277
  add Receiver 103
  manage 277
  Receiver 103
assets
  define old assets 274
  manage 274
  severity 323
  audio files, manage alarm 215
authentication for ePO 142
auto create data sources 69
auto create data sources rules, add 70
auto learning data sources, set up 85
auto-blacklist rules 317
auto-blacklist, configure 150
auto-learned data source rules, manage 296
back up
  ELM 114
  ESM settings 178
  system settings 178
backup files, work with 179
bind components work with 179
blacklist
  add McAfee Network Security Manager entry 152
  configure auto-blacklist 150
  entry, add or delete removed McAfee Network Security Manager 152
  from event in view 248
  global 188
  IPS or virtual device 149
  manage IPS 150
  rules automatically 317
  set up global 189
browse reference from view 248
build, view software 41
bypass NIC
  overview 36, 157
  set up 37, 158
CAC
  add users 175
  authentication 174
  login, set up 175
  settings 175
case management
  pane, show 27, 173
  reports, generate 271
cases
  add 267
  add events to an existing case 268
  close 268
  create from alarm 215
  create from triggered alarm 239
  customize summary 214
  edit 268
  email notification 270
  email selected case 270
  filter 270
  reports, generate 271
  send email when add or change 270
cases (continued)
source events, view 270
status, add 269
status, add or edit 270
view all 270
view details 269
cases pane 26
category
add new tag 322
add new variable 288
edit 322
certificate
install new 162
passphrase, obtain McAfee Vulnerability Manager 151
change history, view for rules 320
Check Point data sources, set up 101
child data sources, add 71
client data sources 72
add 72
locate 72
clock, sync device 161
Collector
SIEM Collector 66
color theme, console 26
Common Criteria configuration 18
common event format data sources 97
communication keys, export and restore 185
compare rule files 320
comparing values on distribution graphs 252
components
add parameters to 307
bind 252
customize 242
example of rule 307
export 250
menu options 248
toolbar 245
view 241
views 241
compression, managing ELM 113
compression, set ELM 113
concurrent devices for network discovery 277
condition, add report 230
configuration files, sync DEM 135
configuration management 275
configuration settings, apply to DEM 136
connections
change with ESM 42
set up McAfee Vulnerability Manager 151
console
add device 23, 31
change appearance 27, 173
color theme 26
diagram 26
timeout 27
case preferences 26
contains filter 230
conventions and icons used in this guide 9
copy and paste rules 314
correlation alarm
include source events 203
correlation data sources 89
correlation engine, ACE 117
correlation event, view source events 64
correlation rules 304
add new 305
add parameters 307
conflicts when importing 316
define custom 310
Threat Intelligence Exchange rules 144
view details
set to show details 305
credentials for ePO 142
credentials, obtain and add rule update 21
custom
type filters 260
custom ASP rules, add 295
custom display, add, edit, delete 24, 47
custom rules
view 314
custom type
add name/value group 265
custom types
add time 265
create 262
name/value 265
predefined 262
customer ID 153
D
DAS, assign to store ELM data 111
data access rules, add or edit 309
data acquisition
enable McAfee Risk Advisor 143
McAfee Risk Advisor 143
data allocation, define limits 171
data enrichment 189
add sources 190
query ePO devices 146
data retention limits, set up 170
data source
out-of-sync with ESM 70
data source rules 296
auto-learned, manage 296
data sources 65
add 65
add ArcSight 96
Index

data sources 65 (continued)
    add child 71
    Adiscon setup 98
    advanced syslog parser 90
    ASP encoding 94
    auto create 69
    auto create rules, add 70
    auto learning, set up 85
    Check Point, set up 101
    client 72
    client, add 72
    client, locate 72
    common event format 97
    configure ePolicy Orchestrator 4.0 96
    correlation 89
    encoding for ASP 94
    IBM ISS SiteProtector 100
    import a list 73
    import spreadsheet 74
    manage 66
    McAfee ePO 99
    migrate to another Receiver 84
    move to another system 84
    Security Device Event Exchange (SDEE) 95
    severity and actions maps 89
    show disabled 27, 173
    spreadsheet to import 74
    supported 87
    syslog relay support 98
    time out of sync with ESM 71
    user-defined types 86
    view files generated 86
    Windows security logs 88
    WMI event log 88

data sources, rule actions 296

data storage
    set up ESM 169
    set up ESM VM 169

data storage, add ELM mirrored 109

data storage, mirroring ELM 108

data storage, preparing to store ELM data 104

database
    audit trails 311
    audit trails, set up rule and report 311
    manage 168
    manage index settings 171
    memory utilization 172
    server, add 140
    status 153

database rules
    add new 305
    logic elements 306
    logical elements, edit 307

date format, change 27, 173

deep packet inspection rules 292
    add 293
    attributes, add 293
    default display type, change 27, 173
    default logging pool, set 38
    default view, change 254
    delete
        custom rules 314
        events or flows 248
        triggered alarm 239

DEM
    add action 136
    advanced settings, configure 135
    configuration settings, apply 136
    database server, add 140
    define actions 136
    edit custom action 137
    rule metric references 300
    rules 299
    sensitive data masks 137
    set operation 137
    summary 12, 54
    sync configuration files 135
    update license 135
    user identification 139

DEM rules
    manage custom 310

DEM-specific settings 134

DESM, summary 12, 54

destination IP addresses, show host name in report 230

device display type, select 24, 48

device group, manage 24, 48

device nodes, delete duplicate 25, 48

devices
    add to console 23, 31
    add URL link 41, 49
    aggregation settings 44, 223
    ASN, define settings 42, 221
    build 41
    change default display 27, 173
    change description 41
    change name 41
    connection with ESM, change 42
    control network traffic 35
    count report 153
    delete 30
    delete nodes 25, 53
    device statistics 39
    disable data sources 27, 173
    display type 30
    display type field 30
    export a key 33
    geolocation, define settings 42, 221
    grant access to 40
    group node, delete 25, 53
devices (continued)
  import a key 33
  IPMI port, set up 158
  key 33
  Linux commands 40
  machine ID 41
  manage keys 32
  manage multiple 49
  manage SSH communication keys 34
  message log 39
  model 41
  monitor traffic 40
  NTP servers 38, 155
  organize 24, 34, 47
  reboot 41
  refresh 53
  serial number 41
  set up events, flows, and logs downloads 42, 220
  software, update 34, 39
  start 41
  status data, download 39
  stop 41
  summary reports 49
  sync clocks 161
  sync with ESM 38
  update software 34, 39
  version 41
  view general information 41
  view log 50
  devices icon, add 30
  DHCP, set up 160
  disable ELM mirroring device 109
  disable SSH communication with ESM 42
  discover endpoints 276
  discover the network 275
  display type, select 24, 48
  distributed ESM
    add filters 141
    properties 141
  distribution graph, compare values 252
  DNA protocol anomalies for ADM rules 133
  documentation
    audience for this guide 9
    product-specific, finding 10
    typographical conventions and icons 9
  download
    events, flows, and logs 42, 220
  downloaded rules, override action 323
  drill down in view 248
  duplicate device nodes, delete 25, 48

E
  edit triggered alarm 239
  ELM
    add iSCSI device for storage 110

ELM (continued)
  add mirrored data storage 109
  add storage device 107
  back up 114
  compression 113
  compression, set 113
  DAS device to store ELM data 111
  define alternate storage location 116
  disable mirroring device 109
  external data storage 110
  faster searches, enable 115
  format SAN storage device to store data 111
  integrity check job 117
  integrity check job, create 117
  integrity check, view results 114
  log data, restore 115
  management database, restore 115
  migrating database 116
  mirrored data storage, add 109
  mirrored management database, replace 116
  mirrored storage pool, rebuild 109
  mirroring data storage 108
  move storage pool 108
  preparing to store data 104
  restore 114
  retrieve data 117
  search job 117
  search job, create 117
  search job, view results 114
  search view 238
  search, enhanced 238
  set up communication with 38
  storage allocation, reduce 108
  storage pool, add or edit 107
  storage usage, view 115
  store logs 106
  summary 12, 54
  sync with device 38

ELM redundancy
  return standby ELM to service 112
  suspend communication with standby ELM
    disable redundancy 112
    view details of data synchronization 112
  switch ELMs 112

ELM settings 103

ELM storage, estimating need 103
email
  case notification 270
  settings 154

email protocol modules for ADM rules 132
enable FIPS mode 19
encoding for ASP data source 94
end station setting for network discovery 277
endpoint discovery 276
ePO
add authentication credentials 143
streaming events, view 55
ePO authentication credentials 142
ePO devices
query for data enrichment 146
query for Real Time for McAfee ePO dashboard 147
query for reports or views 146
ePolicy Orchestrator
configure 4.0 96
launch from ESM 142
McAfee Risk Advisor data acquisition, enable 143
settings 141
tags, assign to IP address 143
ESM
back up settings 178
backup files 179
control network traffic 159
data storage, set up 169
IPMI port, set up 158
logging, set up 184
manage 181
out-of-sync with data source 70
redundant ESM 178
redundant, how it works 180
replace redundant 181
restore settings 179
rules 312
security features 173
summary 12, 54
sync with device 38
time out of sync with data source 71
update software 21
upgrade primary and redundant 186
view system information 153
event forwarding
add destinations 224
add filters 226
agents 225
configure 224
edit filter settings 227
enable or disable 226
modify settings 226
setting up 224
Event Receiver
summary 12, 54
event time report 153
events
add to a case 268
blacklist from 248
check for 221
create a case to track 268
delete 248
description 219
log, manage types of events 183

events (continued)
logs, set language 22, 184
look around for matching fields 253
manage aggregation exceptions 44, 224
mark as reviewed 248
retrieve 221, 222
session details, view 235
set inactivity threshold 220
set up downloads 42, 220
severity weights, set up 324
events, flows & logs
limit collection time 220
exceptions to aggregation settings, add 44, 223
exceptions, add firewall rule 292
export
communication keys 185
component 250
key 33
rules 316
view 248
export and import
exk file 17
puk file 17
export zones 279
external API
manage queries 185, 186
external ELM data storage 110
F
failed Receiver, replace 63
file extensions for export files 15
file maintenance, manage 180
file sharing, disable HomeGroup 106
file transfer protocol modules for ADM rules 132
filter rules
data order 294
rule order 294
Filter rules
set order 295
filter sets
manage 256
filter settings, edit event forwarding 227
filter, contains 230
filters
add rules 294
add to distributed ESM 141
custom type 260
existing rules 317
options, add and remove 256
pane 26
save current values as default 256
toolbar 256
triggered alarm 239
UCF 257
use default 256
filters (continued)  
  user visible and all, switch between 256  
  views 255  
  Windows event ID 257  
filters, event forwarding 226  
FIPS mode  
  backup information 16  
  check integrity 15  
  communicate with multiple ESM devices 17  
  enable 14  
  features available only in FIPS mode 14  
  file extensions 15  
  keyed device, add 15  
  non-compliant available features 14  
  removed features 14  
  restore information 16  
  select 14  
  terminology 15  
  troubleshoot 18  
firewall rules 291  
  access 149  
  add custom 292  
  add exceptions 292  
  create from event or flow 248  
  types 291  
flags, device or system 50  
flow logging, enable 237  
flows  
  check for 221  
  delete 248  
  description 219  
  retrieve 221, 222  
  set inactivity threshold 220  
  set up downloads 42, 220  
  views 237  
G  
geolocation, define settings for device 42, 221  
get event and flows icon 30  
global blacklist 188  
  set up 189  
Global Threat Intelligence watchlist 258  
grids  
  set up users 177  
  users 172  
GTI watchlist 258  
H  
Hadoop PIG 191  
hardware 153  
health monitor  
  signature IDs 206  
  health status flags 30, 50  
hierarchical ESM, mask data 184  
high-availability Receivers 55  
historical correlation events, download 120  
historical correlation, ACE 119  
historical correlation, add filter 120  
history  
  policy change 324  
  view change for rules 320  
HomeGroup file sharing, disable 106  
host names  
  manage 159, 160  
  host names, show in report 230  
I  
IBM ISS SiteProtector data source 100  
images  
  add to login page 20  
  include in PDFs and reports 229  
import  
  data sources list 73  
  device key 33  
  rules 315  
  string normalization file 260  
  variable 288  
import data sources spreadsheet 74  
import zone settings 279  
inactive partitions archive, set up 170  
inactivity threshold, set 220  
index settings, database 171  
indexes, increase available accumulator 169  
indexing, accumulator 171  
informational flags 50  
integrity check job 117  
  create 117  
  integrity check, view results 114  
interface  
  manage network 35, 156  
  network settings 35, 157  
internal rules 293  
  manage 293  
Internet sources  
  create watchlist 258  
IP  
  address, assign ePolicy Orchestrator tags 143  
IP exclusion list, manage 276  
IP protocol anomalies for ADM rules 133  
IPMI port, configure network 158  
IPMI port, set up on ESM or devices 158  
IPS  
  alerts only mode 313  
  analysis report, generate 148  
  anomaly detection variables, edit 148  
  anomaly detection wizard 147  
  auto-blacklist, configure 150  
  blacklist 149  
  blacklist, manage 150
IPS (continued)
  configure settings 147
  internal rules 293
  priority traffic variable 325
iSCSI device, add for ELM storage 110

K
key
device 33
export 33
import 33
manage device 32

L
language, set for event logs 22, 184
launch
ePolicy Orchestrator 248
ePolicy Orchestrator from ESM 142
layout, add report 229
LDAP
  login authentication 174
  server, authenticate users 177
license, update DEM 135
limits, set up data retention 170
link components 252
Linux
  available commands 187
  commands 187
Linux commands, enter for device 40
literals for ADM rules 126
log data, restore ELM 115
logging
  console, first time 19
  enable flow 237
  off console 19
  set the default pool 38
  set up ESM 184
  view system or device 50
logic elements for ADM, database, correlation rules 306
logical elements, edit 307
login
  access control list 174
  define settings 174
  security 173
login page, customize 20
logo, add to login page 20
logs
  check for 221
  description 219
  manage 183
  set language 22, 184
  set up downloads 42, 220
  types to generate 183
logs, store ELM 106
look around for matching fields in events 253

M
machine ID, view device 41
mail server, connect 154
management database, restore ELM 115
map of the network 276
mask IP addresses 184
McAfee ePO
  credentials, set up user 28, 176
McAfee ePO data sources 99
McAfee MIB 164
McAfee Network Security Manager
  add or delete 152
  blacklist entry, add 152
  removed blacklist entry 152
  settings 152
McAfee Risk Advisor
  data acquisition 143
  data acquisition, enable 143
McAfee rulesets 102
McAfee ServicePortal, accessing 10
McAfee Vulnerability Manager
  certificate and passphrase, obtain 151
  connections, set up 151
  run scans 151
  scan, perform from view 248
  settings 151
memory, database utilization 172
message log, view for device 39
message settings 154
metadata events 120
metric references
  ADM rules 130
  DEM rules 300
MIB, McAfee 164
migrate data sources to another Receiver 84
migrating database, ELM 116
mirrored data storage, add ELM 109
mirrored management database, replace ELM 116
mirrored storage pool, rebuild 109
mirroring device, disable ELM 109
mirroring ELM data storage 108
model, view device 41
modify rules 314
monitor device traffic 40
move data sources to another system 84
move storage pool 108
multiple devices
  manage 49
  management icon 30

N
name/value custom types 265
name/value group custom type, add 265
network
  configure settings 155
  interfaces, set for devices 35, 157
  manage interfaces 35, 156
  ports for Receiver-HA 58
  topology component, add devices 243
  topology, device details 244
network discovery 275
  configuration management 275
network discovery stations
  ping sweep interval 277
  ping timeout 277
  subnets to ping 277
network map 276
network settings
  IPMI port set up 158
network traffic control
  devices 35
  ESM 159
Nitro IPS
  summary 12, 54
normalization 312
notification, configure SNMP 37
NSM
  NSM-SIEM configuration tool 99
  streaming events, view 55
NTP servers
  set up for a device 38, 155
  view status 155

O
obfuscation 184
old assets, define 274
operation, set for DEM 137
operators for ADM rules 126
out of sync time between ESM and data source 70, 71
out-of-box views 236
override action on downloaded rules 323
oversubscription mode, set up 313

P
parameters, add to correlation rule or component 307
partitions, set up inactive archive 170
passphrase and certificate, obtain McAfee Vulnerability Manager 151
passwords
  change 27, 173
  default 19
passwords on session viewer, display 122
PDFs, include image 229
ping settings for network discovery 277
policy
  add 285
policy (continued)
  apply changes 325
  child policy, add 285
  copy 285
  delete 285
  export 285
  import 285
  locate 285
  Policy Tree 284
  Policy Tree icons 284
  rename 285
  view rules 285
Policy Editor
  change history 324
  oversubscription mode, set up 313
  view update status for devices 314
ports
  Receiver-HA, network 58
portscan detection 290
predefined views 236
preferences, console 26
preprocessor rules 290
primary ESM, upgrade 186
priority traffic, manager 325
profiles, configure 162
protocol
  anomaly events 120
  protocol anomalies, TCP 289
  protocol-specific properties for ADM rules 132
Q
quarterly reports, set start month 228
queries
  delete running 185, 186
  manage 185, 186
query CSV reports 154
Query Wizard 250
quick launch icons 26
R
RADIUS
  authentication settings 174
  login authentication 174
raw data, archiving 63
Real Time for McAfee ePO
  execute actions 144
  query ePO for dashboard 147
reboot devices 41
rebuild mirrored storage pool 109
Receiver
  asset source, add 103
  data sources 65
  Receiver-HA 55
    check status 61
Receiver-HA 55 (continued)
  network ports 58
  reinitialize secondary device 60
  replace failed Receiver 63
  set up devices 59
  switch roles 60
  troubleshoot failure 63
  upgrade 61

Receivers
  archive settings, define 63
  archiving raw data 63
  asset sources 103
  configure settings 55
  streaming events, view 55

recipients
  add 154
  manage alarm 215

reduce ELM storage allocation 108

redundant ESM
  how it works 180
  replace 181
  save system settings 180
  set up 178
  upgrade 186

reference ADM dictionary 125

refresh devices 53

REGEX grammar for ADM rules 126

reinitialize secondary Receiver-HA device 60

remedy
  case ID, add to event record 249
  case ID, set 248
  server settings 153

remote command profile, configure 162

remote device, access 187

removed McAfee Network Security Manager blacklist entry, add or delete 152

replace failed Receiver-HA 63

report
  manage queries 185, 186

reports
  add 229
  add condition 230
  alarm queue 216
  case management, generate 271
  device summary 49
  ESM device type count 153
  event time 153
  include image 229
  IPS analysis, generate 148
  layout 229
  notifications, add recipients 154
  out-of-box 228
  quarterly, set start month 228
  query ePO devices 146
  show host names 230

reports (continued)
  user-defined 228
  restart multiple devices 49
  restore
    communication keys 185
    system settings 178
  restore backed up configuration files 179
  restore ELM from back up 114
  restore ESM settings 179
  retention, set up data limits 170
  retrieve rule updates 319
  risk
    threats to include in calculation 281
    risk correlation engine, ACE 117
    risk correlation manager, add 119
    risk correlation scoring 119
    risk severity threat management
      managing 280
      views, custom and pre-defined 280
  RPC normalization 290
  rules
    add alarm 204
    add to watchlist 321
    advanced syslog parser 294
    auto-blacklist 317
    check for updates 22
    clear updates status 319
    compare files 320
    copy and paste 314
    create custom from event 248
    data source 296
    delete custom 314
    export 316
    filter existing 317
    firewall, access 149
    history, view change 320
    import 315
    internal 293
    modify 314
    modify aggregation settings 322
    normalization 312
    override action on downloaded 323
    preprocessor 290
    retrieve updates 319
    severity 323
    standard, access 149
    transaction tracking, add or edit 310
    trigger events 120
    types and properties 286
    update credentials 21
    variables 287
    view custom 314
    view signature 319
    Windows events 297
  rulesets 102
SAN storage device, format to store ELM data 111
scans, run McAfee Vulnerability Manager 151
scoring, risk correlation 119
SDEE data sources 95
search ELM 248
search job 117
search job, create 117
search job, view results 114
search, enhanced ELM 238
searches, enable faster ELM 115
secondary Receiver-HA device, reinitialize 60
security features 173
security, SSH communication keys 34
selection rule for virtual devices, manage 46
sensitive data masks 137
manage 138
serial number
view device 41
ServicePortal, finding product documentation 10
session details, view 235
session hijacking, TCP 289
session viewer, display passwords 122
severity
data sources 89
maps 89
weights 323
weights, set up 324
signature IDs for health monitor 206
signature, view rules 319
SNMP
configuration 162
configure notifications 37
MIB 164
power failure notification 163
settings 162
software
update on multiple devices 49
software, update device 34, 39
software, update ESM 21
source events
include in correlation alarm 203
source events, view for correlation event 64
source IP addresses, show host name in report 230
sources, add data enrichment 190
SSH
communication keys, manage for devices 34
communication, disable with ESM 42
regenerate key 185
standard rules, access 149
start devices 41
start multiple devices 49
static routes, add 36, 157
statistics, view for device 39
status
devices, view policy update 314
inactive 50
Receiver-HA 61
status for cases, add 269
status of device, download data about 39
stop devices 41
stop multiple devices 49
storage
set up ESM data 169
set up ESM VM data 169
storage allocation, reduce ELM 108
storage device, add ELM 107
storage pool, add or edit 107
storage pool, add storage device to link to 107
storage pool, move 108
storage pool, rebuild mirrored 109
storage usage, view ELM 115
storage, ELM alternate location 116
store ELM data, preparing to 104
store ELM logs 106
streaming events for Receiver, NSM, ePO 55
string normalization
create file to import 260
manage files 260
subzones
add 280
supported data sources 87
switch Receiver-HA roles 60
sync device
clocks 161
sync device with ESM 38
synchronize system time 161
syslog relay support 98
system clock 153
system log, view 50
system navigation
bar 26
tree 26
system navigation tree
diagram 30
organize devices 34
system settings
back up 178
restore 178
save to redundant ESM 180
T
tagging, ePO 142
tags
add new 322
assign ePolicy Orchestrator to IP address 143
assign to rules or assets 322
category, add new 322
tags (continued)
custom, delete 322
delete custom 322
edit existing 322
severity 323
target-based IP defragmenter 290
target-based TCP reassembly 290
task manager 185, 186
TCP
  protocol anomalies 289
  session hijacking 289
TCP dump, 40
TCP protocol anomalies for ADM rules 133
TCP/UDP session tracking 290
technical support, finding product information 10
templates, add alarm 214
templates, manage alarm 214
term types for ADM rules 128
terminal, use linux commands 187
Threat Intelligence Exchange
  integration with ESM
  execution history 144
threat management 280
threats
  enable or disable for risk calculation 281
  view details 281
TIE execution history 248
time custom types, add 265
time synchronization 161
time zone
  format, change 27, 173
time, synchronize time 161
timeout, console 27
track an event 268
transaction tracking rule, add or edit 310
triggered alarms
  acknowledge 239
  create a case 239
  delete 239
  edit 239
  filter 239
  view details 239
troubleshoot FIPS mode 18
troubleshooting
  Receiver-HA failure 63
types of rules 286

V
VA data, integrate 66
VA data, retrieve 68
VA retrieval, troubleshoot 68
VA source, add 67
VA system profile, define 67
VA vendors available on ESM 69
variables 287
  category, add new 288
  custom, add 288
  delete custom 288
  import 288
  modify 288
  modify type 288
  priority_traffic 325
version, view software 41
view
  manage queries 185, 186
view pane preferences 27
views
  add custom 240
  change default 254
  component toolbar 245
  components 241
  components, customizing 242
  components, description 241
  data details 245
  data in a view 255
  enhanced ELM search 238
  filtering 255
updated rule status, clear 319
updates
  check for rule 22
  retrieve rule 319
upgrade
  primary and redundant ESM 186
  Receiver-HA 61
URL link
  add device information 41
URL links
  add to device 49
user identification
  add rule 139
  manage 139
user-defined data source types 86
users
  add 173
  add CAC login 175
  authenticate to LDAP server 177
  default name 19
  disable 176
  re-enable 176
  working with 172

U
UCF filters 257
update
  software on multiple devices 49
  status for devices, view policy 314
update DEM license 135
update device software 34, 39
update ESM software 21
views (continued)
  filters 255
  flow 237
  host names, display instead of IP address 240
  manage 253
  pane 26
  predefined 236
  query ePO devices 146
  toolbar 26, 235
virtual devices 45
  add to device 47
  alerts only mode 313
  blacklist 149
  internal rules 293
  selection rules, manage 46
VLAN
  add 37, 157
  change 248
VM, set up data storage 169
vulnerability
  assessment 278
  manage sources 278
  severity 323

W
watchlist
  add 258
  add rules 321
  append events to 248
  create in view 248
watchlist (continued)
  create new 321
  GTI 258
  manage queries 185, 186
  overview 257
  Threat Intelligence Exchange watchlist 144
watchlists
  Internet sources 258
web mail protocol modules for ADM rules 132
web request normalization 290
weights, set up severity 324
WHOIS
  lookup from view 248
  lookup, perform 249
Windows
  event ID filters 257
  events rules 297
Windows security logs 88
WMI event log 88
workflow tracking 268

Z
zipzap 290
zone management 278
zones
  add 279
  add a subzone 280
  export settings 279
  import zone settings 279
  manage 278