Contents

Introduction .......................................................................................................................... 7
Using this guide .................................................................................................................. 7
Audience ............................................................................................................................. 7
Find product documentation ............................................................................................ 7

How McAfee Vulnerability Manager works ................................................................. 8
Components and what they do .......................................................................................... 8
How components interact ............................................................................................... 8
Assets that McAfee Vulnerability Manager 7.5 can identify ............................................. 9

Getting started ................................................................................................................. 10
Discovery scans and how they work ............................................................................... 10
Create a discovery scan ..................................................................................................... 10
What you can learn from a discovery report ..................................................................... 10
View a discovery scan report ............................................................................................ 11
Vulnerability scans and how they work ............................................................................ 11
The role of credentials in a vulnerability scan ................................................................. 12
Create a full vulnerability scan ......................................................................................... 12
What you can learn from a vulnerability report ............................................................... 13
View the reports page ....................................................................................................... 13
View a vulnerability scan report ....................................................................................... 14

Monitor the health of your network ................................................................................. 15
How FoundScore® values work ...................................................................................... 15
Customizing FoundScore values for your organization ................................................... 16
How scan reports and custom reports work ..................................................................... 18
Create a custom report ..................................................................................................... 18
View reports ..................................................................................................................... 19
Archive reports ................................................................................................................ 19
How the dashboard work ................................................................................................. 20
Most prevalent vulnerabilities .......................................................................................... 20
Most prevalent operating systems ................................................................................... 20
Vulnerability count by severity ....................................................................................... 21
Vulnerability percentage by severity ............................................................................... 21
Organization vulnerability trend count ......................................................................... 21
Archive asset data ............................................................................................................ 22

Configure McAfee Vulnerability Manager ..................................................................... 23
Role-based access for users ............................................................................................. 23
The purpose of the Global Administrator ........................................................................ 23
View users currently logged into the enterprise manager .................................................. 24
View an activity log for a specific user .............................................................................. 24
How workgroups work .................................................................................................... 25
Create a user ..................................................................................................................... 25
Create a workgroup ......................................................................................................... 26
How scan engines work ................................................................................................... 26
Manage scan engines ....................................................................................................... 27
Modify scan engine settings ............................................................................................ 27
How to use data sources ................................................................................................... 28
Create a McAfee ePolicy Orchestrator data source .......................................................... 30
Use Windows Authentication with a McAfee ePO data source ....................................... 31
Create an LDAP data source ........................................................................................... 31
Create a McAfee Vulnerability Manager data source ....................................................... 33
Schedule a recurring data source .................................................................................... 35
Contents

Working with McAfee Vulnerability Manager Scans ................................. 52
Scan Status page .................................................................................. 52
Scan status descriptions....................................................................... 52
Scan detail descriptions ..................................................................... 53
How the product scans a host.............................................................. 56
How scan configuration settings work ................................................. 57
Create a scan configuration................................................................. 57
Creating credential sets ................................................................... 59
Perform SSH key collection ............................................................... 60
How scan templates work.................................................................. 61
Create a scan with a vulnerability scan template ............................. 61
How to use custom scan templates ..................................................... 62
Create a custom scan template .......................................................... 63
How vulnerability sets work............................................................... 63
Create a Tree Based vulnerability set ................................................. 63
Create a Rule Based vulnerability set ................................................ 65
Modify a vulnerability set.................................................................. 66
Duplicate a vulnerability set............................................................... 67
Delete a vulnerability set................................................................... 67
Add a vulnerability set to a scan configuration ................................. 67
Add a vulnerability set to a custom report ........................................ 67
Check for vulnerability sets in use...................................................... 68
McAfee vulnerability sets.................................................................. 68
Add a McAfee vulnerability set to a scan configuration .................. 69
Add a McAfee vulnerability set to a custom report template ......... 69
Add a McAfee vulnerability set to a scan template ......................... 69
Create a vulnerability set based on a McAfee vulnerability set ....... 69
View McAfee vulnerability sets in use.............................................. 70
Use McAfee vulnerability sets in synchronized data ...................... 70
Vulnerability sets based on CVSS scores .......................................... 71
How XCCDF/OVAL benchmark scans work ....................................... 74
OVAL overview ............................................................................... 74
OVAL links........................................................................................ 75
Working with XCCDF and OVAL ...................................................... 76
Using the United States Federal Information Processing Standard ...... 80
FDCC compliance scans.................................................................... 81
Export Windows Policy settings ......................................................... 81
Import FDCC XML file .................................................................... 81
Run FDCC scan template ................................................................. 81
SUDO scans ...................................................................................... 82
Configure SUDO ............................................................................ 82
Use SUDO in credential sets and scan configurations .................... 83
Oracle on non-standard ports............................................................. 83
Add Oracle on a non-standard port to a scan configuration ............ 83
How web application scans work ....................................................... 84
Create web application configurations ............................................ 84
Create a web application scan ......................................................... 85
Add a web asset............................................................................... 87
Managing remediation and risk ....................................................... 89
Managing notifications.................................................................... 89
How notifications work.................................................................... 89
Unable to view Benchmark Scan reports in the enterprise manager ........................................146

Index.............................................................................................................................................147
Introduction

McAfee Vulnerability Manager is an agentless network scanner that helps you identify and protect the assets (systems) on your network. This allows managers to monitor and respond to changing risks in their environment.

This product guide contains the concepts and tasks that administrators and users need for using the product. Reference material (field and template descriptions) is in the web portal online help. When possible, the online help is context sensitive, and clicking the help icon should display reference material appropriate for the page.

Note: The McAfee Foundstone product is now known as McAfee Vulnerability Manager. For this release, some portions of the product retain the Foundstone label.

Using this guide

This guide helps administrators configure and use the product. The information is organized with frequently used tasks, such as setting up a scan, presented first. Tasks that are used less often, such as database maintenance, appear toward the end of the guide.

Audience

This information is intended for:

- **Network administrators** – Those who are responsible for protecting their network systems from threats, and for managing reports and remediation notifications.
- **Users** – Those who have access to McAfee Vulnerability Manager.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installing to using and troubleshooting.

1. Go to the McAfee Product Download site.
2. Type in your grant number, then click Submit.
3. Select McAfee Vulnerability Manager.

After a product is released, information about the product is entered into the McAfee online KnowledgeBase at http://mysupport.mcafee.com.
How McAfee Vulnerability Manager works

McAfee Vulnerability Manager helps organizations identify and protect the systems (assets) that matter the most on their networks. With the software, administrators monitor their network, respond to vulnerabilities, and adjust to a changing risk environment. The product is an agentless scanner, meaning you do not have to install a software component (agent) on every system in your network.

Components and what they do

McAfee Vulnerability Manager consists of components that work together to monitor your systems.

- **Enterprise manager** – Uses Microsoft Internet Information Services (IIS) to provide authorized users with access to McAfee Vulnerability Manager through their web browsers. It allows them to manage and run the product from anywhere on the network. Access is protected by user identification and authentication. Set up Secure Socket Layers (SSL) through the web server to provide encrypted communication to browsers.

- **Scan engine** – Scans the network environment. Depending on the logistics and size of your network, you might need more than one scan engine to scan the network.

- **Scan controller** – Provides the communication between the scan engine and the database. Most network environments only need one scan controller. For a large network (class A) or segmented network (WAN), use multiple scan controllers.

- **Database** – The data repository for the product. It uses Microsoft SQL Server to store everything from scan settings and results to user accounts and scan engine settings. It contains all of the information needed to track organizations and workgroups, manage users and groups, run scans, and generate reports.

- **API server** – Provides the communication between the enterprise manager and the database.

- **Notification service** – Provides SNMP and email (SMTP) notification messages for integration with third-party help desk management systems and email servers.

- **Data synchronization service** – Gathers information from McAfee ePO databases, LDAP servers, and other McAfee Vulnerability Manager 7.5 databases. For McAfee ePO databases, it provides data to the product for host and OS identification. For LDAP servers, it provides assets you can add to scan configurations. For other McAfee Vulnerability Manager databases, it provides scan data.


- **Configuration manager** – Distributes initial certificates to the other product components and manages the updates to the product components.

- **Web application scanner** – Provides a scan configuration, vulnerability checks, and scan reports for web applications. The web application scanner is a module that must be purchased.

How components interact

Once the product is installed and running, most user interaction is done through the enterprise manager. From the enterprise manager, you can consolidate your organizations, workgroups, and users into logical groups (based on your network needs). The enterprise manager is used to create scan configurations, check on scan status, and view reports.
Assets that McAfee Vulnerability Manager 7.5 can identify

McAfee Vulnerability Manager identifies the following operating systems and other assets in order to determine which scripts to run against the host to check for vulnerabilities. The product can identify the following operating systems:

**Operating systems**
- Berkeley Software Distribution (BSD)
- Red Hat Enterprise Linux versions 3, 4, 5
- SuSE 8, 9, 10
- Sun Solaris versions 7, 8, 9, 10
- IRIX
- Hewlett-Packard HP-UX 10.01, 10.10, 10.20, 11.00, 11.23, 11.31
- IBM AIX versions 5.1, 5.2, 5.3, 6.1
- Macintosh 10.4, 10.5
- Windows NT
- Windows XP
- Windows 2000
- Windows 95
- Windows 98
- Windows ME
- Windows 2003
- Windows 2008
- Windows 7
- Novell
- UNIX
- Cisco IOS versions 11.3, 12.2, 12.3

**Other assets**
- Printer
- Router

The product groups scripts that represent operating systems of a very similar nature. For example, the scripts that run against the Windows operating systems includes scripts for Windows 95, Windows 98, Windows ME, Windows 2000, Windows XP, Windows Vista, Windows 2003, and Windows 2008. UNIX scripts target specific operating systems, such as Linux, Solaris, HP-UX, and AIX. Grouped scripts include the following categories:
- Unknown
- Mac
- Windows
- Shell
- Router
Getting started

The two key tasks in using McAfee Vulnerability Manager are creating scans and reviewing the results of that scan in a report.

Discovery scans and how they work

A discovery scan searches your network for computers and other network devices. These are known as assets. McAfee recommends that you run a discovery scan against a range of IP addresses on your network. This gives you a better idea of what assets the product can discover on your network.

Create a discovery scan

Conduct a discovery scan against the IP address range of your network. A discovery scan only looks for assets on your network.

Checking for vulnerabilities on those assets is not part of a discovery scan. For this reason, you could run a discovery scan against a large network without impacting McAfee Vulnerability Manager performance.

1. Log on to the enterprise manager, then select Scans | New Scan.
2. On the Scan Details page, select Use a McAfee Vulnerability Manager template.
3. Select Asset Discovery Scan, then click Next.
4. On the Targets page, type the Name and an optional Description.
5. Type a starting IP address and an ending IP address for your IP range.
6. Click Add IP Range.
7. On the Scheduler tab, select Active. Immediate, the default selection, means the scan runs after you save it.
8. Click Save and Scan Now.
9. Select Scans | Scan Status to view the progress of this scan configuration.
10. Once the scan is complete, click Reports in the Actions column, then click View Report.

Note: You can also select Reports | View Scan Reports to view scan reports.

What you can learn from a discovery report

A discovery report has information about the number of active systems, operating systems, and network services discovered within the given IP range.

Scan Reports page

The reports page shows the latest three jobs generated for a particular scan created by your organization/workgroup. Showing three reports on this page makes it easy to compare the differences and note any progress.
Scan reports page descriptions

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan selection</td>
<td>Lets you select the scan you want to view from the scan drop-down box.</td>
</tr>
<tr>
<td>Completed reports</td>
<td>Shows custom reports or scan reports.</td>
</tr>
<tr>
<td>View report</td>
<td>Opens the HTML report for the scan.</td>
</tr>
<tr>
<td>General</td>
<td>Lists the number of vulnerabilities discovered by this scan, the number of live hosts, and services.</td>
</tr>
<tr>
<td>Top services</td>
<td>Lists the top three services discovered by the scan. This list displays how many times the service was discovered and then the service name.</td>
</tr>
<tr>
<td>Top vulnerabilities</td>
<td>Lists the top three vulnerabilities discovered by the scan. This list displays the how many times the vulnerability was discovered and then the vulnerability name.</td>
</tr>
</tbody>
</table>

Note: Discovery scans do not check for vulnerabilities.

Download lets you select the report format to download.

View a discovery scan report

Once your first discovery scan is complete, you can view the results in the web browser by going to the reports page.

1. Log on to the enterprise manager, then select Reports | View Scan Reports.
2. Select a discovery scan from the scan selection drop-down list, then click View Report.
3. Scroll down to the Discovered Hosts Summary section. This shows you the total number of active hosts found and the number of IP addresses scanned during the discovery scan.
4. Click the IP range. The Hosts Report page appears.
5. Click the plus sign to expand the list of active hosts. All of the assets discovered during the discovery scan appear on the Active Hosts list.

Note: You can use the report navigation bar to change the number of rows or view a specific page.

Vulnerability scans and how they work

A vulnerability scan searches selected systems on your network for known vulnerabilities, such as whether a service pack installed. A vulnerability scan can return all scan data (Vulnerable, Not Vulnerable, or Indeterminate) or only Vulnerable data. Indeterminate scan data is often the result of a system being inaccessible.
The role of credentials in a vulnerability scan

Including credentials in your scan configuration allows McAfee Vulnerability Manager to log on to systems in your network. This provides a better understanding of where a system is vulnerable to attacks.

This feature lets you add different methods of authentication to access an account on a host:

- Windows Domain
- Windows Workgroup
- Windows Individual Host
- Windows Default
- Shell Domain
- Shell Individual Host
- Shell Default
- Web Domain
- Web Server
- Web Default
- Web Application URL

Each method of authentication requires a user ID (user name), and some methods require a password. The database stores the encrypted user names and passwords for this scan. When the scan begins, the product uses this information to attempt authentication on each discovered host system.

**Caution:** When you set up credentials, make sure they comply with your network security policies. It is possible to provide multiple credentials with the same user name. When the product tries each of these credentials, it might surpass the limits allowed by your network policy without warning, possibly resulting in locked accounts on scanned hosts.

Create a full vulnerability scan

Run a full vulnerability scan that targets a small set of systems on your network. By scanning a small set of systems, your first scan should finish faster and produce a full vulnerability scan report for you to review.

1. Log on to the enterprise manager, then select **Scans** | **New Scan**.
2. On the **Scan Details** page, select **Use a McAfee Vulnerability Manager template**.
3. Select **Full Vulnerability Scan**, then click **Next**.
4. On the **Targets** page, type the **Name** and an optional **Description**.
5. Specify IP address, IP range, or URL to be scanned, then click **Next**.

**Note:** Scanning a URL requires the web application scanner.

6. On the **Settings** page, click the **Credentials** icon on the left side of the page to add credentials to this scan configuration.
   a. Select **Domain/Workgroup**.
   b. Domain credentials are recommended, but providing credentials depends on your company’s policies.
   c. Type a unique name for this scan configuration in the **Domain/Workgroup** field.
   d. Type the user ID and password.
   e. Click **Add/Update** to add this credential to the scan configuration.

**Note:** For more information about credentials in a scan configuration, see The role of credentials in a vulnerability scan (page 12).
Getting started
What you can learn from a vulnerability report

7 Click Next.
8 On the Reports tab, select HTML for your first vulnerability scan.
9 Click Next to go to the Scheduler tab.
10 On the Scheduler tab, select Active. Immediate, the default selection, means the scan runs after you save it.
11 Click Save and Scan Now.
12 Select Scans | Scan Status to view the progress of this scan configuration.
13 Once the scan is complete, click Reports in the Actions column, then click View Report.

Note: You can also select Reports | View Scan Reports to view scan reports.

What you can learn from a vulnerability report

A vulnerability report provides summary information for what was discovered during the scan, with detailed information about each scanned system and each detected vulnerability.

A vulnerability report has information about the number of vulnerabilities found on the active systems scanned. View the vulnerabilities by severity (risk level), by individual IP address (showing all the vulnerabilities discovered for that IP address), and by operating system.

View the reports page

The reports page shows the latest three jobs generated for a particular scan created by your organization/workgroup. Showing three reports on this page makes it easy to compare the differences and note any progress.

Scan reports page descriptions

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan selection</td>
<td>Select the scan you want to view from the scan drop-down box.</td>
</tr>
<tr>
<td>Completed reports</td>
<td>Select to view custom reports or scan reports.</td>
</tr>
<tr>
<td>View report</td>
<td>Click to open the HTML report for the scan.</td>
</tr>
<tr>
<td>General</td>
<td>Lists the number of vulnerabilities discovered by this scan, the number of live hosts, and services.</td>
</tr>
<tr>
<td>Top services</td>
<td>Lists the most common services discovered by the scan.</td>
</tr>
<tr>
<td>Top vulnerabilities</td>
<td>Lists the top vulnerabilities discovered by the scan.</td>
</tr>
</tbody>
</table>

Note: Discovery scans do not check for vulnerabilities.

Download Click the report format you wish to download.
View a vulnerability scan report

Once your first vulnerability scan is complete, you can view the results in the web browser by going to the reports page.

1. Log on to the enterprise manager, then select Reports | View Scan Reports.
2. Make sure your vulnerability scan is selected in the scan selection drop-down list.
3. Click View Report.
4. Scroll down to the Vulnerability Report Summary section. This section shows you the top vulnerabilities discovered on the asset scanned during your vulnerability scan.
Monitor the health of your network

In addition to reports, McAfee Vulnerability Manager provides metrics, dashboards, and scan results that help you view changes in your network security over time.

How FoundScore® values work

McAfee Vulnerability Manager uses an algorithm called a FoundScore value to describe how vulnerable your network is to known threats. The FoundScore value ranges from 0 to 100, with a higher FoundScore value representing a more secure network.

There are two types of FoundScore values, an internal and an external. The internal value is based on internal attacks made on your network. The product imitates the efforts of an attacker looking for internal vulnerabilities and exposures on the network. The external value is based on external attacks made on your network and the product imitates the efforts of an attacker looking for external vulnerabilities and exposures.

\[
\text{[vulnerability score]} + \text{[exposures score]} = \text{FoundScore value}
\]

<table>
<thead>
<tr>
<th>Default scores</th>
<th>Internal FoundScore value</th>
<th>External FoundScore value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>70</td>
<td>50</td>
</tr>
<tr>
<td>Exposures</td>
<td>30</td>
<td>50</td>
</tr>
<tr>
<td>Total Score</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

Vulnerability score

Modify a vulnerability score by using the MyFoundScore value.

The minimum FoundScore value is 0. If a network has a large number of vulnerabilities and exposures, it might take considerable effort to resolve them to get the FoundScore value above 0.

The vulnerability score is based on the combination of high, medium and low risk vulnerabilities discovered within your environment. Points are deducted for each vulnerability found, based on its risk ranking (high, medium, low).

High risk

An attacker might gain privileged access (administrator, root) to the system over a remote connection.

Examples:

- IIS Remote Data Services provides remote control
- RPC Auto-mounted attack

Medium risk

An attacker might gain non-privileged (user) access to the system over a remote connection.
Monitor the health of your network

How FoundScore® values work

Examples:

- ColdFusion viewexample.cfm
- Open and accessible NetBIOS ports

**Low risk**

The vulnerability provides enticement data to the attacker that can be used to launch a more informed attack against the target environment. It can indirectly lead to some form of remote connection access to the system.

Examples:

- Anonymous FTP access
- Easy-to-guess SNMP community string

**Informational risk**

Available data that is less valuable to an attacker than the low risk vulnerability. You might also not be able to address informational findings; they might be inherent to the network services or architecture in use.

For example, an informational vulnerability might include gaining access to data using NetBIOS name table retrieval (NBTStat). However, the ability to enumerate Windows user accounts via a null session is a low vulnerability.

You might not be able to address informational findings — they might be inherent to the network services or architecture in use. For example, the SSH protocol requires a version number, support cipher and methods exchange to be included in the service banner.

**Customizing FoundScore values for your organization**

You can change the metrics used to calculate a MyFoundScore value. Changing these metrics allows you to increase or decrease the importance of a vulnerability found on a system based on the Asset Criticality level assigned to the system.

1. Log on as the Root Organization Administrator, then select **Manage | Metrics**.
2. Type in your MyFoundScore custom settings.
3. Click **Submit**.

**MyFoundScore General tab**

- To customize the criticality multiplier that McAfee Vulnerability Manager uses to calculate your FoundScore value, use a MyFoundScore value. Set **Use MyFoundScore** to **Yes**. Then change the criticality multiplier as needed in the Custom column.
- To return adjusted criticality multipliers to the last saved setting, click **Reset**.
- The valid range of numbers for the Custom Criticality Multiplier is 0-100. If 0 is used, the criticality is ignored. A custom multiplier set to 1 means the criticality level is low, while setting it to 100 means the criticality level is high.

**Note:** To configure the FoundScore value so that it takes asset criticality into consideration, you must first assign criticality levels to your assets (see "Viewing asset properties" on page 40). Otherwise all assets use the multiplier of 1.
General tab settings

- **Use MyFoundScore** – To enable custom settings used to calculate MyFoundScore values throughout the reports for this organization, select **Yes** from the drop-down list. If **No** is selected, the reports and summaries show the default FoundScore value.

- **Default vs. Custom (column headings)** – The default value shows you what the product uses to calculate the regular, default FoundScore value. If Use MyFoundScore is set to **Yes**, the product uses the **Custom** settings to calculate MyFoundScore values.

- **Asset Criticality** – These are the criticality ratings that can be assigned in Asset Management. By default, all assets are counted as **Moderate**, and have a multiplier of 1. Asset Criticality does not affect the FoundScore value until you change the criticality of specific IP addresses or groups in Asset Management.

  If an asset is not assigned a criticality, its rating is automatically set at 0.

**FoundScore External or Internal tabs**

- To customize the deductions used to calculate your FoundScore values, use MyFoundScore values. Set **Use MyFoundScore** to **Yes**. Then change the deduction as needed in the Custom column.

- To return all modified deductions to the last saved setting, click **Reset**.

Vulnerability Deduction descriptions

- **Maximum Deductions Total** – This setting determines the maximum number of deductions that can be taken for Vulnerabilities. The default is set at 50 points, meaning that external vulnerability risks have the same weight as external exposures (also 50 points).

  If you change the weighting for this setting, make sure that the maximum deductions for Exposures and this score total 100 points.
Monitor the health of your network
How scan reports and custom reports work

- **Each High/Medium/Low Risk Vulnerability** – Change the number of points that should be deducted for each level of vulnerability risk discovered in your environment. Setting **Each High Risk Vulnerability** to the maximum number automatically deducts all possible vulnerability points. This reflects the seriousness of the vulnerability discovered.

  **Note:** Each Risk Vulnerability number has a valid range of 0-100 and the Risk Vulnerability number must be less than or equal to the Maximum Deductions number. For example, the Maximum Deductions for Vulnerabilities is 50, each Risk Vulnerability can be 0-50.

**Exposure Deduction descriptions**
- **Maximum Deductions Total** – The maximum number of points to deduct based on exposure.
- **Maximum Deductions Non-Essential Services** – The maximum number of points to deduct for non-essential services.
- **Each Discovered Non-Essential Service** – The number of points to deduct for each non-essential service discovered by the scan.
- **Maximum Deductions Machines Without an Essential Service** – The maximum number of points deducted for systems discovered without an essential service.
- **Each Machine Without an Essential Service** – The number of points to deduct for each system discovered without an essential service.
- **UDP Permitted Other Than Port 53 (DNS)** – Typically UDP services are not required for systems exposed to the external internet, with the exception of DNS on port 53. Typically UDP services are not required on systems exposed to external scans. UDP is a security exposure because it is a common transport protocol for popular Denial of Service attacks and backdoor programs such as trin00 and Back Orifice. In addition, the connection-less nature of UDP complicates monitoring and auditing UDP-based services.
- **ICMP Permitted Inbound** – Although useful for simple diagnostic testing, permitting inbound ICMP traffic creates significant exposure because attackers use it for popular Denial of Service attacks such as mstream and Tribal Flood Network.

---

**How scan reports and custom reports work**
Scan reports show the results of your vulnerability scans. Custom reports show information about specific systems and network components.

**Create a custom report**
Creating a custom report template allows you to generate a report that contains the data (single date, trend data), the system information (operating system, organization), and the report sections (asset details, FoundScore) that you want to review.

**Note:** Asset-based reports always use the Internal FoundScore value.

1. Select **Reports | Generate Custom Reports**.
2. Click **Create New Template**.
3. Type a unique name in the **Name** field and an optional **Description**.

  **Tip:** Periodically save your settings by clicking **Save**, in the unlikely event that something happens with your Internet browser.

4. On the **Report Type** tab, select a report type.
   - Select a report type, **Vulnerability Report**, **Compliance Report**, **PCI Report**, or **XCCDF Report**.
   - Select **Single Date Report**, **Delta Report**, **Trend Report**, or **Dashboard Report**.
5 Select the appropriate date (or dates) for the selected report type.

**Tip:** Select **Use Most Recent Data** to report on the most recent data available.

6 On the **Asset Filter** tab, select the criteria to be used in your report.
   - To add a condition, click **Add Condition**.
   - To add a nested condition, click **Add Nested Condition**.
   - To edit a condition, click **Edit this Condition**.
   - To change the AND / OR operators, click the operator.
   - To delete a condition, click **Delete this Condition**.
   - To delete a condition group, click **Delete this Condition Group**.
   - To move a condition, drag and drop the condition to the desired location.

7 On the **Sections** tab, select the report sections to include in your report.

8 On the **Generation** tab, select the report formats, language, include the report template settings, and schedule for the report.

9 On the **Delivery** tab, add the roles and email addresses that should receive the report each time it is generated.

10 Click **Save**.

### View reports

For scan reports, you can view the results in the web browser once the scan is complete. For custom reports, you must create and execute a custom report template first.

**Custom Reports**
- To view a custom report, select **Reports | View Custom Reports**.
- Download a custom report by clicking on a report icon.
- View a custom report by clicking on the report name.

**Scan Reports**
- To view a scan report, select **Reports | View Scan Reports**.
- To view the results from a different scan, select the scan from the drop-down box in the upper-right corner.
- To view a full list of scans, click `...` next to the scan drop-down box in the upper-right corner.
- Download or view available reports for the various scan jobs.

### Archive reports

Storing your old reports on your report server could impact performance. McAfee recommends storing your archived reports to another location, like a network folder.

**Note:** On the server running the report engine, the default report folder location is C:\Program Files\Foundstone\Reports.
How the dashboard work

The dashboard provides summary information for vulnerabilities, operating systems, severity, and vulnerability count trending.

- **Most Prevalent Vulnerabilities** – Shows the ten vulnerabilities that affect the most number of assets in your organization or group.
- **Most Prevalent Operating Systems** – Shows the ten operating systems used the most on assets in your organization or group.
- **Vulnerability Count by Severity** – Shows the number of High, Medium, Low, and Informational vulnerabilities, based on all of the assets in your organization or group.
- **Vulnerability Percentage by Severity** – Shows the total percentage of High, Medium, Low, and Informational vulnerabilities affecting assets in your organization or group.
- **Organization Vulnerability Count Trend** – Shows a trend graph of the High, Medium, Low, and Informational vulnerabilities affecting assets in your organization or group.

Most prevalent vulnerabilities

This monitor shows the ten vulnerabilities with the highest number of occurrences, based on the minimum severity level selected.

Clicking on a vulnerability displays the Vulnerability Details page.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset count</td>
<td>The number of assets the vulnerability was discovered on.</td>
</tr>
<tr>
<td>Chart/List view</td>
<td>Changes the display to either a bar chart or a list.</td>
</tr>
<tr>
<td>Minimum severity</td>
<td>Displays the vulnerabilities with the selected severity level or higher.</td>
</tr>
<tr>
<td></td>
<td>Example: Selecting Med displays the medium and high severity level vulnerabilities discovered on the highest number of assets.</td>
</tr>
<tr>
<td>Vulnerability name</td>
<td>The name of the vulnerability.</td>
</tr>
</tbody>
</table>

Most prevalent operating systems

This monitor shows the ten operating systems with the highest number of occurrences, based on scanned assets.

Clicking on an operating system displays the Asset Management page, with search results based on the selected operating system.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset count</td>
<td>The number of assets the vulnerability was discovered on.</td>
</tr>
<tr>
<td>Chart/List view</td>
<td>Changes the display to either a bar chart or a list.</td>
</tr>
</tbody>
</table>
Monitor the health of your network
How the dashboard work

### Vulnerability count by severity

This monitor shows the number of High, Medium, Low, and Information vulnerabilities. This chart displays archived data and is updated once every 24 hours. You can update this view using the Archive Asset Data (page 22) feature using the configuration manager.

Clicking on a severity level displays the Vulnerabilities by Severity page, with the severity level information expanded.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>The name and version of the operating system.</td>
</tr>
</tbody>
</table>

### Vulnerability percentage by severity

This monitor shows the percentage of High, Medium, Low, and Information vulnerabilities. This chart displays archived data and is updated once every 24 hours. You can update this view using the Archive Asset Data (page 22) feature using the configuration manager.

Clicking on a severity level displays the Vulnerabilities by Severity page, with the severity level information expanded.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current as of</td>
<td>Displays the date and time the information was updated.</td>
</tr>
<tr>
<td>Severity</td>
<td>A bar chart representation of the number of High, Medium, Low, and Information vulnerabilities.</td>
</tr>
<tr>
<td>Vulnerability count</td>
<td>Displays the number of vulnerabilities.</td>
</tr>
</tbody>
</table>

### Organization vulnerability trend count

This monitor shows a trend graph of the High, Medium, Low, and Information vulnerabilities, over time. This chart displays archived data and is updated once every 24 hours. You can update this view using the Archive Asset Data (page 22) feature using the configuration manager.

**Note:** If you upgraded to McAfee Vulnerability Manager 7.5, the product calculates the current data for the organization and display that information on the first day of the upgrade.

Placing the mouse pointer over a data point in the graph displays the severity level, the date the information was posted to the dashboard, and the number of vulnerabilities.
The Vulnerability Counts and Foundscores trend graphs are updated when there is new data, like when a system changes or a new scan is run. On days when there is no new data, the trend value is the same as the previous value.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current as of</td>
<td>Displays the date and time the information was updated.</td>
</tr>
<tr>
<td>Date</td>
<td>Displays the date the information was posted to the dashboard.</td>
</tr>
<tr>
<td>View Foundscores</td>
<td>Clicking on the link displays the trend graph based on the Foundscore.</td>
</tr>
</tbody>
</table>

**Note:** If you upgraded to McAfee Vulnerability Manager 7.5, previous releases displayed Foundscore values based on a scan, now the values are based on assets. There could be a difference between your old Foundscore values and your new values.

<table>
<thead>
<tr>
<th>View Vulnerability Counts</th>
<th>Clicking on the link displays the trend graph based on severity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability counts</td>
<td>Displays the number of vulnerabilities.</td>
</tr>
</tbody>
</table>

**Archive asset data**

Archiving asset data helps with database maintenance. The product archives asset data once a day. You can manually archive data using the configuration manager.

On the dashboard, the Vulnerability Count by Severity, Vulnerability Percentage by Severity, and Organization Vulnerability Count Trend views display information from the archived asset data. If you run scans daily, there could be some differences between data on the dashboard views, the Vulnerabilities by Severity page, and the Asset Search page (which uses data from the latest scan). For example, differences could result if assets are deleted, scans are run, and the asset data hasn't been archived.

1. On the server running the configuration manager, select Start | All Programs | Foundstone | FCM Console.
2. Select Tools | Preferences.
3. Click the Database tab.
4. Select Run Now for Archive Asset data, then click Apply.
5. Click OK, then close the configuration manager. The amount of time it takes before the archived asset data is available for the dashboard depends on the size of your database.
Configure McAfee Vulnerability Manager

As the Root Organization Administrator, you can add scan engines and external data sources, as well as maintain your asset (system) information.

Role-based access for users

McAfee Vulnerability Manager controls access to information based on users' roles. These roles are implemented through the enterprise manager.

Administrative roles

- **Global Administrator** – The Global Administrator is a built-in role. The password is set during installation. It is used to set up one or more top-level organization, and create the Root Organization Administrator for each organization. The Global Administrator can also set up workgroups under an organization, and can create users and user roles.

  **Note:** If you are logged on to the enterprise manager as a Global Administrator and want to view data from a specific organization, you must log off and log back on as a Root Organization Administrator for that organization.

- **Root Organization Administrator** – The Root Organization Administrator is created by the Global Administrator. The Root Organization Administrators have full access to their assigned organization and any workgroups within their organization. They manage assets, scan configurations, user accounts, remediation tickets, and scan engines.

  **Note:** The Root Organization Administrator manages the scan engine settings (see "How scan engines work" on page 26) from the enterprise manager. Workgroup Administrators do not have access to scan engine settings.

- **Workgroup Administrator** – The Workgroup Administrator is created by the Global Administrator or Root Organization Administrator. The Workgroup Administrators has full access to their assigned workgroup and any sub-workgroups within their own workgroup. They manage assets, scan configurations, user accounts, and remediation tickets.

- **Remediation Administrator** – The Remediation Administrator is created by adding users to the built-in Remediation Administrator group. This person can manage remediation tickets for the entire organization.

  Administrators can change the access rights for specific users or user groups to provide additional levels of access.

The purpose of the Global Administrator

The Global Administrator's actions affect all organizations and workgroups. The Global Administrator can create new organizations or workgroups, view all users currently logged on to the web portal, and create new scan templates.
View users currently logged into the enterprise manager

The Global Administrator can view a list of users currently using the enterprise manager. The Global Administrator can terminate the user sessions for maintenance purposes.

The log out function does not instantly terminate a user session. After the Global Administrator terminates a user session, the user's next action returns the session to the logon page. This action does not prevent the user from logging back on.

If you need to terminate user sessions and keep users from entering the enterprise manager, you can force the user to log out and then lock them out. By locking out a user, you can keep the user from entering the enterprise manager. Unlock the users to allow them to log back on.

1. Log on as the Global Administrator, then select Manage | Active Sessions.
2. On the Active Sessions page, click Log out to log off a user.

Active Sessions
- **User ID** – Displays the user ID for all accounts currently logged on to the enterprise manager.
- **Organization** – Displays the name of the organization associated with the user.
- **IP address** – Displays the IP address of the user.
- **Last Activity** – Displays the date and time of the user's last action in the product.
- **Action - log out** – Allows you to remotely log off the selected user.

View an activity log for a specific user

The product logs actions from each workgroup and user account. View the logs for any user account that you can access.

- To see the user activity log file, right-click the user and click View Logs.
- To sort the log, click a column heading in the log file.

The Activity Logs window displays information for the selected user.

1. Log on to the enterprise manager, then select Manage | Users/Groups.
2. Select the user whose log you want to view.
   You might need to expand the organization or workgroup the user belongs to.
3 Right-click the user and select **View Logs**.

![Activity Logs - shows account activity](image)

Log features
- **Date/time** – The date and time of the event.
- **Organization** – The organization or workgroup name associated with the user.
- **User name** – The logon user name for the account that ran the event.
- **IP address** – The IP address of the host that ran the event.
- **Description** – Describes the event that took place.

---

### How workgroups work

Root organization administrators can group their users and assign permissions to those groups. Workgroups can also be used to group systems for scanning.

### Create a user

Use this task to create a McAfee Vulnerability Manager user and assign a workgroup and role. Global Administrators, Root Organization Administrators, and Workgroup Administrators can create new users.

1 Right-click the organization or workgroup, then select **New | User**. The **User Information** window appears.

2 Type the user information, then select **Next**. The required fields are marked with an asterisk (*) and red typeface until their individual requirements have been met.
Under **Available Roles**, select the role to apply to this user. Selecting the administrative role gives the user administrative privileges to that organization or workgroup.

![Figure 3: User Account properties – Member of tab](image)

1. Click **Add** to add the group to the **Member Of** column.
2. Click **Next**.
3. On the **Scan Access Rights** page, you can modify the access rights for this user. When you are done, click **Finish**.

### Create a workgroup

Create workgroups to organize your users or to group systems for specific scans. Use workgroups to organize your IP range into manageable segments, so multiple administrators can manage the scanning and remediation process while reports and demographic information flow up through the hierarchy for review.

1. In the hierarchical organization tree view, right-click the workgroup or organization under which you want to create the new Workgroup, then from the shortcut menu select **New | Workgroup**. The New Workgroup page appears.
2. Type the new workgroup Name and Description and click **Finish**.

**Note:** Workgroups must contain unique names. Do not create a workgroup using the name of an existing workgroup.

3. To edit the workgroup properties, right-click the workgroup and select **Properties**.

### How scan engines work

A scan engine is a key component to McAfee Vulnerability Manager because it gathers information from systems on your network. If you have more than one scan engine, a list of the available engines appears on the Scan Schedule page so that you can select the system that should run the scan.

**Note:** If you create multiple root organizations, they should use separate engines or at least have a common administrator that knows to avoid overlapping settings. The engine settings can be edited by any Root Organization Administrator.
Manage scan engines

After adding a scan engine, you can manage it through the McAfee Vulnerability Manager web interface as the Global Administrator or Root Organization Administrator.

The settings on this page affect the entire organization, including all workgroups. Workgroup administrators cannot make changes to these settings.

- To change the Description, make the change and click **Update**.
- To modify the engine preferences, click **Preferences**.

**Note:** If an engine is supposed to appear on this list but does not, make the engine available in the Organization or Workgroup Properties.

Scan engine settings

- **Name** – Provides the ability to type a descriptive name for the scan engine. The name and description are stored in the engine registry.
- **Description** – The optional description can provide additional information about the location or purpose of this scan engine. Click **Update** to accept any changes you make.
- **Type** – Displays the type of system on which the scan engine is running. If the product is running on a McAfee appliance, it appears here. If it is running on customer-supplied equipment, **Custom** appears.
- **Status** – Shows whether the scan controller is communicating with this scan engine. If the status is online, the scan controller is able to communicate with the scan engine. This status is updated every 30 seconds as the database polls each engine.
- **Action**
  - **Update** – Click **Update** to submit changes to the scan engine.
  - **Delete** – Removes this scan engine from the list. Engines that are online cannot be deleted from the list.
  - **Pause engine/Resume engine** – Pauses all scans on this scan engine (Global Administrator only).
  - **Preferences** – Edit the settings for this engine.
  - **Refresh** – Refreshes the engine list to display the latest settings.

Modify scan engine settings

While scan engines have default settings, your network configuration might require you to modify those settings.
Engine preferences – Network options

To have the engine detect whether it is connected to the network, select Enable Network Connectivity Detection. Type at least one IP address in the New Target IP field and click Add.

![Figure 4: Engine Preferences – Network Options](image)

Network Connectivity Detection settings

- **Enable network connectivity detection** – Turn this feature on to ping a reliable host to ensure that the scan engine is connected to your network as it scans. If it is not connected, it cannot find any hosts and reports no vulnerabilities on your network.

  If the network is inactive or erratic, the product pauses all scans until network connectivity is re-established or stabilized.

- **New target IP** – Enter the IP address of a reliable host and click Add. The target is added to the Ping Targets list.

- **Ping targets** – This list shows the IP addresses that the scan engine can ping to ensure that it is connected to the network. You can remove items from this list by selecting the item and clicking Remove.

- **Timeout** – Type how many seconds (1 – 10) to wait for a response to the ping.

- **Interval** – Type how often (1 – 100) you want to send the ping to verify that the scanner is online.

- **Threshold** – Type how many times (1 – 10) the ping should fail to pause the scans running on this engine. McAfee Vulnerability Manager 7.5 continues sending a ping to the target, and resumes the scans when the ping threshold is no longer breached.

---

How to use data sources

McAfee Vulnerability Manager provides a data synchronization service that allows the product to use data from a McAfee ePolicy Orchestrator database, from Lightweight Directory Access Protocol (LDAP) servers, or from other McAfee Vulnerability Manager 7.5 databases.

**Note:** McAfee Vulnerability Manager 7.5 can scan IPv6 addresses, but does not support IPv6 addresses for synchronizing with data sources.

McAfee Vulnerability Manager 7.5 supports McAfee ePolicy Orchestrator 4.5, McAfee ePolicy Orchestrator 4.6, LDAP version 3 and 4 (with Generic, NTLM, and Simple access), and McAfee Vulnerability Manager 7.5 databases.
You can incorporate data from different sources to provide more details about the assets on your network. You can also provide asset information from other databases that are gathering data from a remote site or for a site that is not accessible (like an air-gapped network). You can then use this information when generating reports. Setting up data sources is ideal for gathering data. Resolving vulnerabilities through ticketing is best done on the McAfee Vulnerability Manager system that originally scanned the asset.

If your active directory domain is configured to use Secure Sockets Layer (SSL) encryption, ensure the system hosting the Data Synchronization Service has the requisite certificates in place.

The product adds the following information to the reports, which show assets with McAfee ePolicy Orchestrator data:

- Operating system
- Service pack level

When importing data into McAfee Vulnerability Manager:

- McAfee ePolicy Orchestrator data is given a higher priority over existing operating system information in the database.
- When importing data from another database, tickets are recreated when the import is done. If the same asset has data in both databases, some tickets might be automatically closed based on the asset data being imported.

**Note:** The LDAP server must support "paged search control."

**Using the data source page**

- **Add Data Source** – You can add a McAfee ePolicy Orchestrator Data Source (page 30), LDAP Data Source, or McAfee Vulnerability Manager Data Source (page 33).
- **Edit** – Allows you to edit an existing data source.
- **Delete** – Use this to delete a data source (page 36).
- **Test** – Use this to see if the product can connect to the data source (page 36).

**Data source settings**

- **Name** – Descriptive name
- **Server address** – IP address or fully-qualified domain name
- **Type** – McAfee ePolicy Orchestrator, McAfee Vulnerability Manager, or LDAP server
- **Last sync time** – Date and time of the last successful synchronization
- **Last sync status** – Status of the last synchronization
- **Next sync time** – Date and time of the next synchronization
- **Actions** – Edit, Delete, or Test the database connection
- **Add data source** – Specify the location and settings for a new McAfee ePolicy Orchestrator database
- **Refresh** – Refreshes the page to update the information
Create a McAfee ePolicy Orchestrator data source

You can import data from your McAfee ePO database into McAfee Vulnerability Manager and synchronize the information about systems on your network.

**Note:** If you must use Windows Authentication for synchronizing data with a McAfee ePO database, see Using Windows Authentication with a McAfee ePO server data source (page 31).

1. Select **Manage | Data Sources**.
2. Click **Add Data Source**.
3. Type a name in the **Name** field.
4. Select **ePO** from the **Data Source Type** list.
5. Type the IP address of the McAfee ePO database.
   - If the McAfee ePO database does not use the default instance name (e.g. MSSQLSERVER), you can specify the instance name in this field (e.g. 123.45.67.89\EPOSERVER). For ports other than 1433, include the port number (e.g. 123.45.67.89:123\EPOSERVER).
6. Type the name of the McAfee ePO database.
7. Type a user name and password.
   - The user name must have at least read-access to the McAfee ePO database.
   - If you are using Windows Authentication, the user name format must be user@domain or domain\user.

![Figure 6: McAfee ePO server data source options](image)

---

Configure McAfee Vulnerability Manager
How to use data sources

McAfee Vulnerability Manager 7.5 Product Guide 30
For McAfee ePolicy Orchestrator and McAfee Policy Auditor integration, select **Enable Audit Request**. The **McAfee Vulnerability Manager Organization/Workgroup** list appears.

Select the organization or workgroup from the drop-down list.

Select **Active** or **Inactive** for the **Scheduler**.

Select a **Schedule Type** (**Immediate** or **One Time**) or a **Recurring** (**Daily**, **Weekly**, **Monthly**). Refer to Scheduling a recurring data source (page 35).

Note: If you select **Daily**, **Weekly**, or **Monthly**, also select the appropriate **Schedule** options for this data source.

Click **Save**, then click **Exit**.

On the **Data Source** page, you can test your data source connection.

### Use Windows Authentication with a McAfee ePO data source

To use Windows Authentication when synchronizing data from a McAfee ePolicy Orchestrator database to McAfee Vulnerability Manager, there are some additional requirements.

- The data synchronization service must be added to the same domain as the McAfee ePO database.
- On the server hosting the McAfee ePO database, the domain account must be a credentialed account in Microsoft SQL Server and must have read privileges to the McAfee ePO database.
- The domain account used in the McAfee ePolicy Orchestrator data source must have the ability to log on to the server hosting the data synchronization service. The account must be added to the Local Users and Groups of the server. If the domain account is either Guest or User, then enable the Allow log on locally policy for the account. If the account is an Administrator or Power User, there is no need to enable this policy.

### Create an LDAP data source

You can import data from your LDAP server into McAfee Vulnerability Manager and synchronize the information about systems on your network.

1. Select **Manage | Data Sources**.
2. Click **Add Data Source**.
3. Type a name in the **Name** field.
4. Select **LDAP** from the **Data Source Type** list.
5. Type entries for these options:
   - **LDAP IP address or fully-qualified domain name (FQDN)**
   - **LDAP server port number**
   - **Timeout number in seconds (optional)**

Note: A fully-qualified domain name is required if you are using an SSL connection.
Configure McAfee Vulnerability Manager
How to use data sources

32

Note: Timeout determines how long the data synchronization service waits for a reply from the LDAP server before deciding that the LDAP server is not responding. If this field is left blank, the data synchronization service uses the server default.

Figure 7: LDAP data source connection properties

6 Select a connection type.
Select SSL if your LDAP server supports it. If not, leave the selection as Standard.

7 Select an authentication type (NTLM, Generic, or Simple).
If you are using OpenLDAP, you must use Simple authentication. Simple authentication requires the user name follow the format cn=User,ou=People,o=Company. For example: cn=Manager,dc=organizationdomain,dc=com.

Note: NTLM and Generic authentication are not compatible with LDAP in Linux environments.

8 Type the domain that the LDAP data source belongs to.

9 Type a user name and password.

Figure 8: LDAP data source connection properties

10 The LDAP Search Root is a string that specifies the root of the LDAP tree. For the LDAP Search Root, specify where asset searches should begin.
Example: dc=organizationdomain, dc=com

Note: The fields in the LDAP Attribute Mapping are case-insensitive.
The LDAP Search Filter sets criteria that helps reduce the number of attributes returned by a search.
Example: (objectclass=computer) imports all computers from the LDAP server to the Faultline database.

Note: To import an OU structure, specify the root of the OU structure as your LDAP root and use an LDAP filter to remove any results that should be synchronized.

11 Type entries for these options:
• **NetBIOS Name** – LDAP attribute containing the NetBIOS name
Configure McAfee Vulnerability Manager
How to use data sources

- **DNS Name** – LDAP attribute containing the host (Domain) name
- **IP Address** – LDAP attribute containing the IP Address
- **Domain Name** – LDAP attribute containing the DNS Name (if it exists)
- **MAC Address** – LDAP attribute containing the MAC address (if it exists)

*Note:* The values in the LDAP Attribute Mapping are given by the administrator, and could vary from system to system.

12 Select **Active** or **Inactive** for the **Scheduler**.
13 Select a Schedule Type (**Immediate** or **One Time**) or a Recurring (**Daily**, **Weekly**, **Monthly**).

*Note:* If you select **Daily**, **Weekly**, or **Monthly**, also select the appropriate Schedule options for this data source.

14 Click **Save**, then click **Exit**.
15 On the Data Source page, you can test your data source connection (page 36).
16 After your LDAP data source is synchronized successfully, you can add your LDAP assets to your scan configurations. On the Targets tab of a scan configuration, click **Browse** and then select your LDAP data source from the Asset Source list. For more details on adding assets to your scan configuration, click the help icon when adding targets to a scan configuration.

*Note:* If you need to view or troubleshoot the data retrieved from the synchronization, create a scan and browse your LDAP assets. You can also view the LDAPAssets table in the database for more information.

Create a McAfee Vulnerability Manager data source

You can import data from other McAfee Vulnerability Manager 7.5 databases and generate reports.

*Note:* The McAfee Vulnerability Manager versions must be the same, including any patches.

1 Select **Manage | Data Sources**.
2 Click **Add Data Source**.
3 Select **McAfee Vulnerability Manager** from the **Data Source Type** list.
4 Type a name in the **Name** field.
5 Type entries for these options:
   - McAfee Vulnerability Manager server address or fully-qualified domain name (FQDN)
     Once a McAfee Vulnerability Manager data source is saved, this field cannot be edited. You must create a new McAfee Vulnerability Manager data source to correct a server address or FQDN error.

*Note:* A fully-qualified domain name is required if you are using an SSL connection.

- McAfee Vulnerability Manager database name
Configure McAfee Vulnerability Manager
How to use data sources

- User name, password, and source organization/workgroup for the data you want to import

6 Select the target organization or workgroup to import the data into. Your organization and any workgroups in your organization appear on the drop-down list.

7 The Advanced feature allows you to import McAfee Vulnerability Manager data based on a date range (start time and end time) instead of importing all of the data for the source organization or workgroup. Select Enable, then select a Start Time and End time dates and times. If you do not enable this function, all of the data available for the source organization or workgroup is imported. The scan time applies to the data in the data source, not the McAfee Vulnerability Manager database importing the data.

8 Select Active or Inactive for the Scheduler.

9 Select a Schedule Type (Immediate or One Time) or a Recurring (Daily, Weekly, Monthly). See Scheduling a data source (page 35).

   **Note:** If you select Daily, Weekly, or Monthly, also select the appropriate Schedule options for this data source.

10 Click Save, then click Exit.

11 On the Data Source page, you can test your data source connection (page 36).
Schedule a recurring data source

By scheduling a recurring data import from an external source, you can automate the frequency that McAfee Vulnerability Manager imports and synchronize the data.

Set up a Daily Recurring Data Source
1. Under **Recurring**, select **Daily**
2. Type the **Start On** date.

   **Note:** You can also use the Calendar to select a start date.

3. Select an hour and minutes to run this data source on a daily basis.

   **Note:** The schedule uses Coordinated Universal Time (UTC), which might be different from your local time.

4. Click **Save**.

Set up a Weekly Recurring Data Source
1. Select **Weekly** under **Recurring**.
2. Select a day of the week to run this data source.

   **Note:** It is possible to select more than one day to run a data source.

3. Select a **Start On** day or select a date to run the scan.
4. Select an hour and minutes to run this data source on a weekly basis.

   **Note:** The schedule uses Coordinated Universal Time (UTC), which might be different from your local time.

5. Select the number of weeks this data source is to recur. For example, selecting 3 means the selected data source runs once every 3 weeks.
6. Click **Save**.

Set up a Monthly Recurring Data Source
1. Select **Monthly** under **Recurring**.
2. Add a **Start On** date.
   - To start on a day during the week, select the week (e.g. First) and the day (e.g. Wednesday).
     Selecting a day and week that do not exist in all months means the data synchronization is skipped for that month (e.g. most months do not have a Fifth Friday).
     Click **Add** to add a **Start On** date.
   - To start on a set day during the month, select **Date** then select a number (e.g. 15th).
     Selecting a number that does not exist in all months means the data synchronization is skipped for that month (e.g. selecting 30th means no data synchronization in February).
     Click **Add** to add a **Start On** date.
3. Select an hour and minutes to run this data source on a monthly basis.

   **Note:** The schedule uses Coordinated Universal Time (UTC), which might be different from your local time.

4. Select the number of months this data source is to recur. For example, selecting 3 means the selected data source runs once every 3 months.
5. Select a **Start Date** for the data synchronization to begin on.
6. Click **Add**. The schedule criteria are added to the list.

   **Note:** You can add more than one schedule criteria to the monthly schedule list.
Remove a data source

You can remove a data source from McAfee Vulnerability Manager when you no longer need it.

**Note:** Deleting a McAfee ePolicy Orchestrator or LDAP data source also removes the asset information from the product. McAfee ePolicy Orchestrator and LDAP assets are removed from all scan configurations.

1. Select **Manage | Data Sources**.
2. Click **Delete** in the row of the Data Source to be deleted. A message appears asking for a confirmation for the deletion.
3. Click **OK**.

Test a data source

You can test the communication between your data source and McAfee Vulnerability Manager to ensure you can import your data. Use this feature before you synchronize with your data source.

1. Select **Manage | Data Sources**.
2. Click **Test** in the row of the Data Source connection to be tested.
   - If you receive a successful test result, your connection is successful.
   - If you receive a failed test result, your connection fails.
   - If your data source is not properly set up, edit your data source.

How to manage assets

McAfee Vulnerability Manager allows you to rate and identify systems throughout your organization. Your FoundScore value can also reflect the ratings you assigned. This lets you place more emphasis on important assets, ensuring that your remediation efforts are prioritized the way you want them. For example, if a production server is compromised, your company is likely at greater risk than if someone were to attack the mailroom postage computer.

Asset properties and asset groups are shared throughout the organization. All workgroups that share an asset can view the same information. The organization can access all assets.

Whether you can view an asset or not depends on the IP addresses you can access. Root Organization Administrators can see assets belonging to the entire organization since all workgroups contain subset IP addresses of the organization itself.
**Note:** Asset criticality does not affect the FoundScore value calculation until you start assigning criticality levels to your assets.

**Tip:** For Microsoft Internet Explorer 8.0, turn off **Display intranet sites in compatibility View**.

## Using the Asset Management page

Organize your assets into groups. This includes creating new groups in a hierarchal structure, and assigning assets to those groups.

- Assign asset labels and criticality levels to individual hosts. To do this, right-click the asset and select **Properties**. Then edit the asset properties (see "Viewing asset properties" on page 40).
- Search for assets by clicking the Search tool on the Asset toolbar (see "Using search options" on page 38). You can run a simple or an advanced search.
  
  When browsing the organization (root node), only assets that are not part of a workgroup (subgroup) are shown in the results.

The buttons and commands on the toolbar let you access the various features of asset management.

Select **Manage | Assets** to go to the Asset Management page.

- **Select Columns** – Displays columns that you can view or hide.
- **Parent Asset Group** – Removes search results and displays all assets in the group.
- **Toggle Tree** – Select an organization or workgroup for managing assets.
- **Asset Search** – Perform a Simple or an Advanced Search of the assets you can access.
- **Show** – Select to display All Assets or only Live Assets.
  - **All Assets** – Displays all assets, whether active or not, labeled or not
  - **Live Assets** – Displays assets that were identified as active in the last scan
- **Page** – Displays the page number being viewed, the total number of pages, and the total number of records. You can scroll to other pages by using the `<prev` or `next>` links.
- **Per page** – Sets the number of records viewed per page. Viewing a higher number of records might cause longer times for the page to refresh.
- **With all search results** – Applies any of the following (when selected after a search) to all assets in the search results.
  - **Add Tag** – Select **Asset Tag**, then select a tag to assign to the selected assets.
  - **Remove Tag** – Removes all asset tags from the selected assets.
  - **Move to Group** – Select **Move to Group**, then select a group from the group list (on the left, under the Search link). This moves all assets in the search results to the selected asset group.
  - **Remove from Group** – Select **Remove from Group** to remove all assets in the search results from the asset group. Assets cannot be removed from the root organization.
  - **Mark as Trusted** – Adds the asset to a list of trusted (verified) hosts.
  - **Remove Trust** – Removes the asset from the list of trusted (verified) hosts.
  - **Delete** – Select **Delete** to delete the assets in the search results from the database. A message appears, requiring you to confirm deleting the assets.
  - **Owner** – Assign an owner to the selected assets. Click the arrow and select the asset owner from the list.
  - **Criticality** – Assign a criticality level to the selected assets. Criticality levels indicate how important this asset is to your business, and the impact to your business should this asset be compromised.
- **Change Start Page** – Allows you to set the page that displays when you log in.
Using asset options

When you right-click an asset, these options can be applied to the asset. You can apply asset options to multiple assets by using the Shift or Alt keys while selecting assets.

- **Move to group** – Select **Move to Group**, then select a group from the group list (on the left, under the Search link). This moves the asset to the selected asset group.
- **Remove from group** – Select **Remove from Group** to remove the asset from the asset group. Assets cannot be removed from the root organization.
- **Delete** – Deletes the asset from the database. A warning message appears to confirm deleting the asset.
- **Properties** – View the asset properties (IP address and label). You can set the criticality level and the owner for the asset.
- **Quickscan** – Starts a quick scan of the selected asset. You can only run one quick scan at a time.
- **Asset details** – Displays the asset details.
- **Mark as trusted** – Adds the asset to a list of trusted (verified) hosts.
- **Remove trust** – Removes the asset from the list of trusted (verified) hosts.

Using search options

The search options let you filter your assets based on criteria that you are looking for. You can perform a simple or an advanced search.

**Use a simple search**

Use a simple search for the asset type, asset status, or criticality filter.

1. Select **Manage | Assets**, then click **Search**.
2. Select **Simple Search**.
3. Type the information you want to search for in the **Search For** field.
4. Select the type of asset information from the **In** drop-down list.
5. Select the asset status you want to include in your search.
6. You can select a criticality filter to apply to your asset search. This filters for assets by the criticality level assigned to it. Criticality levels are manually assigned to an asset.
7. Click **Submit**.

**Use an advanced search**

Use an advanced search to add custom criteria to your search.

1. Select **Manage | Assets**, then click **Search**.
2. Select **Advanced Search**.
3. Select an asset information type from the drop-down list.
4. Select a search parameter from the drop-down list.
5. Type the information you want to search for.
6. Click the **Add Criteria** button to add the search criteria to your list. You can add more search criteria to your list.
7. Select **Match ALL Selected** if all of your search criteria must be met when searching for assets. Select **Match ANY Selected** if you want to see which assets match any of your search criteria. Be sure to select the search criteria you want to use in your search.
8 Select the asset status you want to include in your search.
9 You can select a criticality filter to apply to your asset search. This filters assets by the assigned criticality level. Criticality levels are manually assigned to an asset.
10 Click Submit.

Using group options

In the left pane of the Asset Management page is a list of groups. When you right-click a group name, a list of group options appears.

- **New group** – Adds a new group under the selected group.
- **Move to group** – Allows a group to be moved to another group.
- **Delete** – Deletes the group.
- **Properties** – Displays the properties for the selected group.
- **Add assets** – Allows assets to be added to the group.

Add a new group
1 Right-click the group you want to add a subgroup to.
2 Select New Group.
3 Type a group name.
   You can also select a Criticality level and Owner for this group. The criticality level defines how important the assets in this group are to your business. The higher the impact to your business should these assets be compromised should raise the criticality level you assign.
4 Click Submit.

Move a group
1 Right-click the group you want to move.
2 Select Move to Group.
3 Select the group in the left pane you want to move the selected group to.
   You might need to collapse and expand the parent group to see the group you moved.

Delete a group
1 Right-click the group you want to delete.
2 Select Delete. A message appears, asking you to confirm deleting the selected group.
3 Click OK to delete the group.

View group properties
1 Right-click a group.
2 Select Properties.
   You can change the criticality level and group owner. Changing the group criticality level does not change the criticality level assigned to assets currently in the group; it only affects assets added to the group after the criticality level has been changed. To apply the new criticality level to all assets currently in the group, select Apply this criticality to existing child assets.
3 Click Submit.

Add assets
1 Right-click a group.
2 Select Add Assets.
3 Type an IP address, IP range, or URL.
4 Click Submit.
Viewing asset properties

Asset properties define a system, allowing you to add labels, identify how critical the system is to your organization, and assign a specific user as the owner.

Use the asset properties pane

1. Select Manage | Assets.
2. Right-click an asset and select Properties.
3. View the latest information discovered for a specific host by selecting the host and looking at the properties. The information includes the label, criticality, and asset owner. Web assets include entry paths, exclude paths, exclude parameters, and port pairs.
4. Change a label to a host by typing the new label information in the Label text box. If no label is assigned, the default AssetID appears as the label. You can change the label on one asset at a time.
5. Set the criticality level for the host or IP range by selecting the level from the Criticality list.
6. Assign an Asset Owner to the host or IP range by selecting the user from the Asset Owner list.

![Figure 12: Asset management – Asset properties dialog box](image)

Asset properties

- **IP Address** – Displays the IP address scanned to identify the asset.
- **Label** – Use this field to assign the group or host label. This can be anything you want. If a custom label has not been assigned, the label uses the McAfee Vulnerability Manager Asset ID number for its label.
- **Criticality** – Click the arrow and select the criticality level from the list.
- **Asset owner** – Click the arrow and select the asset owner from the list.

Managing asset identification rules

Asset identification rules help you organize rules for identifying systems on your network into Windows-based systems, non-Windows-based systems, and unknown hosts.

Using the Managing Asset Identification Rules pane you can do the following:

- Create prioritized rules for identifying unique assets.
- Determine the priority for each set of rules.
- View current rule configurations.

The following conditions apply when using asset identification rules:

- Asset identification rules affect the entire organization.
- Asset identification rules affect scans created after the rule was created or edited. Prior scans are not affected.
- Asset identification rules are not applied to existing assets, only to assets found in scans after the rules are applied.
For Windows and Unknown assets, the first rule is preset to identify hosts with McAfee ePolicy Orchestrator UIDs and McAfee Vulnerability Manager Asset ID.

For each asset, the product tries each rule until it finds a rule whose conditions match the asset. Once a rule matches an asset, the remaining rules are ignored.

You can set up multiple rules to identify all the assets on your system.

Each rule contains one or more conditions.

### Use asset identification rules

Use asset identification rules to organize assets on your network.

1. Select Manage | Assets, then click Manage Asset Identification Rules.
2. To set up a rule, select the checkboxes on a single row to select the conditions for that rule. For example, with Windows Assets, McAfee ePolicy Orchestrator UID is automatically selected as the first rule. On row 2, select the checkboxes that correspond to the conditions that should exist in the second rule.
3. To review the rule list, see the text under Configured Rules just below each selection table.
4. To set a limit on how long an undiscovered asset can remain in the product without being labeled as inactive, change the Asset Activity setting at the bottom of the page.

**Note:** You can search for inactive assets using the Advanced Search feature in Asset Management.

### Unique identifier features

Use asset identification rules to control how detected hosts are recognized across scans.

- **Windows Asset** – An asset running a Windows operating system.
- **Non-Windows Asset** – An asset running a non-Windows operating system.
- **Unknown Asset** – An asset with an OS-type that cannot be identified.
- **ePO UID** – The ePolicy Orchestrator unique identifier comes from the McAfee agent running on Windows-based hosts. They are always unique, and provide the most reliable way to identify an asset. The product always looks for an ePolicy Orchestrator identifier on Windows-based hosts.
- **FS Asset ID** – If Asset Tagging is enabled for a scan, the product uses a unique McAfee Vulnerability Manager Asset ID on discovered hosts. In subsequently scans, this ID is used to uniquely identify the host. This improves the accuracy of asset reconciliation across scans.
- **MAC Address** – Address tied to the network adapter (NIC) on the host. It is not solely reliable in asset identification because the network card can be moved to another host.
- **DNS Name** – Use a domain name as part of the unique identifier. Adding this option along with an IP address allows for cases where the same IP address might exist in two different domains.
- **IP Address** – Use an IP address as part of the unique identifier.
  - In a DHCP environment, a rule that contains only this condition can cause confusion if an asset receives a different IP address from DHCP. Be sure to use other conditions along with this rule to ensure you have identified unique assets.
  - In a non-DHCP environment, set up the last rule with this condition to catch all assets that don't match the conditions in previous rules.
- **NetBIOS Name** – In Windows-based systems, use the hostname as part of the unique identifier.
- **Confirmed** – Displays the number of confirmed and unconfirmed assets for each rule selected. Also presents the number as a percentage of the total found for a rule. Running a new scan updates this column.
- **Rule Set Quality** – Displays the percentage of confirmed and unconfirmed assets.
- **Configured Rules** – Displays the order the rules are applied to assets.
- **Asset Activity** – The number of days an asset can go without being discovered or scanned before it is labeled as inactive.
Asset tags and organizing assets

Organization administrators can create and assign a tag to an asset. This allows organization administrators to organize their assets with similar tags, simplifying the performance of some actions.

Organization administrators create static asset tags and apply them manually to assets. Tags can be created based on an operating system (like Windows or Ubuntu), department (like warehouse or finance), or even location (like North America or Europe). Multiple tags can be applied to an asset, or multiple assets, to help narrow the search when looking for specific assets.

For example, using multiple asset tags, administrators can tag all Windows assets that belong to the finance department located in North America.

Dynamic asset tags use a query based on asset filters. Running the query applies the dynamic asset tag to assets that meet the filter criteria. Assets can be filtered by operating system, how important the asset is to the company (asset criticality), and the severity of a vulnerability found on the asset. Administrators can filter for all Windows assets with a high criticality level that have one or more severe vulnerabilities.

Static asset tags

Static asset tags are labels that organization administrators create to organize assets by operating system, department, or location.

Static asset tags can be applied to a single asset or multiple assets. Administrators can search or browse for assets in a scan configuration, generate a custom report, and manage assets based on the asset tag.

Note: If an asset tag is applied to multiple assets that include web application assets, the asset tag is not applied to the web application assets. This also applies to the With all search results feature.

Create static asset tags

Organization administrators can create static asset tags that can be manually applied to an asset or multiple assets.

1. In the enterprise manager, select Components | Asset Tags.
2. Type the name of an asset tag in the text box.
3. To enter more than one asset tag, press the Enter key and type the next asset tag.
4. Click Add.

The Existing Asset Tags list is sorted alphabetically.

Apply static asset tags

Once static asset tags have been created, organization administrators can apply a static asset tag to assets to improve results of searching or browsing for assets.
1. In the enterprise manager, select **Manage | Assets**.

2. Search and select the assets you want to tag. You can select more than one asset on a page, or click **With all search results** and apply the tag to all assets across all search result pages.

3. Right-click and select **Add Tag**.

4. Select an asset tag or multiple tags to apply to the asset(s), then click **Submit**.

---

### Edit static asset tags

Organization administrators can rename a static asset tag. When a static asset tag is renamed, all assets using that tag are updated, including scan configurations, custom report templates, and any asset tags that reference the updated asset tag.

1. In the enterprise manager, select **Components | Asset Tags**.

2. Under **Existing Asset Tags**, select the asset tag to rename.

3. Click **Rename Selected Tag**.

4. Type a name for the asset tag, then click **Rename**.

---

### Delete static asset tags

Organization administrators can delete static asset tags. When a static asset tag is deleted, the asset tag is removed from all assets using that tag. In a custom report or a dynamic asset tag referencing the static asset tag, deleted tags appear as `<Deleted Asset Tag>`.

1. In the enterprise manager, select **Components | Asset Tags**.

2. From the **Existing Asset Tags** list, select one or more asset tags.

3. Click **Delete Selected Tags**, then click **OK** to confirm.

---

### Dynamic asset tags

When creating a dynamic asset tag, organization administrators add asset filters to a query. When the query runs, the name of the dynamic asset tag is applied to any asset that meets the conditions of the asset filters. Dynamic asset tags are applied automatically or manually (page 44).

Dynamic asset tags can be used in scan configurations, custom report templates, referenced in another dynamic asset tag, or searching for assets.

In these instances, a dynamic asset tag could impact performance (complex dynamic asset tag):

- You have a large number of assets (over 50,000).
- You store a large amount of data in your database (like storing all vulnerability results).
- You run large dynamic asset tag queries (applying over 20 asset filters); this includes referencing dynamic asset tags within dynamic asset tags.

Be aware of these conditions:

- If manually applying a dynamic asset tag takes longer than 10 minutes, the query might have timed out. To check if applying the tag succeeded, search for assets you know meet the asset filter conditions. Before searching for assets, make sure the dynamic asset tag is set to manual, otherwise the dynamic asset tag query runs during the asset search.
- A dynamic asset tag is a database query, so applying a complex dynamic asset tag and running other database procedures (scans, reports, web portal) could impact database performance.
• When using a dynamic asset tag in a scan configuration, the tag is applied to all assets included in the scan, not just the ones that were live when the scan was run or could be scanned by the assigned scan engine.

**Note:** Dynamic asset tags are not applied to web application assets.

---

**Create dynamic asset tags**

Organization administrators can create dynamic asset tags that can be used in scan configurations, custom report templates, or are referenced in another dynamic asset tag.

**Note:** In Microsoft Internet Explorer, the Internet security settings for Internet and Local Internet must be set to default for the rule pop-up window to be displayed.

1. In the enterprise manager, select **Components | Asset Tags**.
2. Click the **Dynamic** tab, then click **Create New**.
3. Type a name in the **Tag Name** field.
4. **Optional.** Deselect **Enable Automatic Tagging** and run the dynamic asset tag manually. See **Automatic versus manual dynamic asset tags** (page 44).
5. Click **Add Condition** or **Add Nested Condition**.
6. Select a condition from the list.
7. Select criteria for the condition, then click **Set Condition**.
8. Click **Save**.

**Note:** After you create or modify a dynamic asset tag, run it manually. See **Updating a dynamic asset tag manually** (page 45).

---

**Automatic versus manual dynamic asset tag updates**

When a dynamic asset tag is set to **Enable Automatic Tagging**, the asset tag is updated every time it is used in a scan configuration, custom report template, or asset search.

A task can take significantly more time if:

• The dynamic asset tag is applied to more than 50,000 assets.
• Asset filter conditions are complicated, as in returning all vulnerabilities.

In these cases, organization administrators can deselect Enable Automatic Tagging and update the dynamic asset tag when needed. See **Updating a dynamic asset tag manually** (page 45).

We recommend that organization administrators should apply a dynamic tag immediately after creating it. This applies the tag to assets and indicates how long the tag takes to update. If the tag updates quickly, automatic tagging shouldn't impact the time it takes to perform scans, reports, or asset searches. If the tag takes a long time to update, this tag should be updated manually to save time.

The automatic dynamic asset tag has a default setting where it doesn't run again if less than 10 minutes has elapsed since the tag was last run. This reduces the possibility of having multiple users trying to update the same query within a short period of time. If an update is needed within the 10 minutes, organization administrators can manually apply the asset tag. Editing a dynamic tag resets the 10 minute time limit.

Updating a dynamic asset tag is also affected if it is referenced by another dynamic asset tag, and if the dynamic asset tags are set to update automatically or manually.
Example
Tag A is set to Auto and references Tag B and Tag C.

Tag B is set to Manual and references Tag D. Tag D is set to Auto.

Tag C is set to Auto and references Tag E, Tag F, and Tag G. Tags E and G are set to Auto. Tag F is set to Manual.

Viewed as a hierarchy, it looks like this.
- Tag A (a)
  - Tag B (m)
  - Tag D (a)
  - Tag C (a)
    - Tag E (a)
    - Tag F (m)
    - Tag G (a)

When Tag A is updated, only Tags C, E, and G are updated. Because Tag B is set to Manual, both Tag B and Tag D are not updated. Tag F is set to Manual and is not updated.

When Tag B is manually updated, Tag D is updated.

When Tag C is updated, Tags E and G are updated.

Tag F must be updated manually.

Updating goes from the bottom up, so updating Tag A updates Tags E and G, then Tag C, and finally Tag A.

In this example, since tags E and G are on the same level, there is no priority in updating Tags E and G.

Update a dynamic asset tag manually

When a dynamic asset tag is set to update automatically, the query runs every time the tag is used. For a large number of assets, updating the dynamic asset tag might take a long time to finish. This adds time before a scan or custom report finishes.

For a large number of assets, organization administrators should manually update the dynamic asset tag before running a scan configuration or custom report that contains this asset tag. This gives organization administrators control over when a dynamic asset tag is updated, instead of updating every time it is used.

Every time the dynamic asset tag is updated, the tag looks only for changes since the last time the tag was updated.

Organization administrators can also update a dynamic asset tag manually that has the Enable Automatic Tagging option enabled.

1. In the enterprise manager, select Components | Asset Tags.
2. On the Dynamic tab, click Apply for the dynamic asset tag you want to update. A message reports that the tags are being updated.
**Edit dynamic asset tags**

When the organization administrator edits dynamic asset tags, the asset tag is updated the next time it is applied or used.

1. In the enterprise manager, select **Components | Asset Tags**.
2. Click **View/Edit** for the tag you want to modify.
3. Update the dynamic tag options. You can change the name of the dynamic asset tag, and the change is applied where the tag is used. You can also add or remove asset filters.
4. Click **Save**.

**Delete dynamic asset tags**

Organization administrators can delete dynamic asset tags. When a dynamic asset tag is deleted, the asset tag is removed from all assets using that tag. In a custom report or a dynamic asset tag referencing the asset tag, deleted tags appear as `<Deleted Asset Tag>`.

1. In the enterprise manager, select **Components | Asset Tags**.
2. On the **Dynamic** tab, click **Delete** for the dynamic asset tag you want to delete.
3. Click **OK** to confirm the deletion.

**Duplicate a dynamic asset tag**

Duplicating a dynamic asset tag allows organization administrators to start with an existing set of conditions and modify it to create a new one.

1. In the enterprise manager, select **Components | Asset Tags**, then click the **Dynamic** tab.
2. Click **View/Edit** for the dynamic asset tag you want to duplicate.
3. Click **Save As**. The dynamic asset tag is duplicated, and "Copy of" is added to the beginning of the name.
4. Type a unique name for the dynamic asset tag.
5. Add or remove conditions as needed, then click **Save**.

**Asset filter conditions**

Adding asset filter conditions allows you to specify which assets you are looking for based on selected conditions.

Adding a lot of conditions or IP addresses to the asset filter could make the resulting filter file too large to use. Here are some restrictions and suggestions when using asset filters.

- A maximum of 15 conditions is allowed in a dynamic asset tag. Attempting to add more than 15 displays an error message when you try to save the tag. If you are using the Expression list to keep track of the number of conditions, remember that the numbering starts with 0, not 1.
- When you enter or import IP addresses for an asset filter condition, the dynamic asset tag doesn't allow a large number of IP addresses. If you are receiving error messages when you try to save the tag, try creating an asset group.

The following table describes the options and conditions available for use in an asset filter.

---

**Note**: A user can include only assets that the user can access.
Dynamic asset tag options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add condition</td>
<td>Add a condition at the current level in the hierarchy.</td>
</tr>
<tr>
<td>Add nested condition</td>
<td>Create a new condition on a new child-level in the hierarchy. Nested conditions share the same operator.</td>
</tr>
</tbody>
</table>
| And / Or                    | Toggle between AND and OR. It affects all conditions within the same hierarchical level.  
                              |  • AND: search for any record containing all of the conditions specified in the nested group.  
                              |  • OR: search for any record containing any of the conditions specified in the nested group. |
| Delete this condition       | Remove a condition from the criteria list.                                   |
| Delete this condition group | Remove the conditions contained within a group.                             |
| Edit                        | Open the Edit Condition dialog box and make changes.                        |
| Enable automatic tagging    | The asset tag is updated every time it is used in a scan configuration, custom report template, or asset search. |
| Expression                  | Generate a summarized expression of the conditions entered in this filter.  
                              | Each condition is represented by a number in the expression.                |
| Tag name                    | The name of the dynamic asset tag.                                          |

Conditions and their descriptions

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| Asset Criticality          | Filter assets by criticality level: None, Low, Limited, Moderate, Significant, or Extensive. 
                              | Select to include or exclude the designated levels. Select multiple levels of criticality to include in a report. |
| Asset Group Name           | Filter assets by the group name of a given asset. 
                              | Select to include or exclude the group name from the report. Enter partial information and select whether the selection starts or ends with the partial information. |
| Asset Label                | Filter assets by the label of a given asset.                                |
| Asset Owner                | Enter an owner's name (exact or partial entry) for this filter. Select a setting to either include or exclude any assets associated with the owner for the report; or whether the owner's name starts or ends with the partially entered name. |
## Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Status</td>
<td>Filter assets by the status of an asset. An asset can be Active, Inactive, or Undiscovered. Undiscovered means the asset was added manually but has not been discovered by a scan.</td>
</tr>
<tr>
<td>Asset Tag Set</td>
<td>Filter assets by an asset tag.</td>
</tr>
<tr>
<td>Authentication Status</td>
<td>Filter assets based on the success or failure of WHAM or SSH authenticated access.</td>
</tr>
<tr>
<td>Banners</td>
<td>Filter assets by banner information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Some banner information might contain non-printable characters or line feeds, and might fail to give the expected results.</td>
</tr>
<tr>
<td>CVE Number</td>
<td>Enter a CVE (Common Vulnerabilities and Exposures) number to filter by a specific vulnerability.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Multiple CVE numbers can be added to a condition by separating each number with a comma.</td>
</tr>
<tr>
<td>False Positives</td>
<td>Filter assets by those that have at least one false positive associated with it, or have no false positives associated with it.</td>
</tr>
<tr>
<td>FSL Output</td>
<td>Enter the FSL (Foundstone Scripting Language) output for this filter. Select a setting to include or exclude any assets associated with the FSL Output entered; or whether the FSL Output starts or ends with the partially entered text.</td>
</tr>
<tr>
<td>Host DNS Name</td>
<td>Set this filter to include or exclude any assets with a specific Host DNS name; or whether a Host DNS name starts or ends with the partially entered text.</td>
</tr>
<tr>
<td>Host NetBIOS Name</td>
<td>Set this filter to include or exclude any assets with a specific Host NetBIOS name; or whether a Host NetBIOS name starts or ends with the partially entered text.</td>
</tr>
<tr>
<td>IAVA Number</td>
<td>Enter the IAVA (Information Assurance Vulnerability Alert) number for this filter. Select a setting to include or exclude any assets associated with the IAVA number; or whether the IAVA starts or ends with the partially entered text.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Multiple IAVA numbers can be added to a condition by separating each number with a comma.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP Address(es) or IP Address Range for this filter. It is also possible to import the IP Addresses from a file; the file format must be comma-separated. The maximum file size allowed is 128 KB. Select a setting to either include or exclude the IP Address(es) from the report. Note: While you can enter any IP Address(es) or IP Address Range, your level of access affects which IP Addresses show up in the report.</td>
</tr>
<tr>
<td>KB Number</td>
<td>Enter the Microsoft KnowledgeBase ID Number(s) for this filter. Numbers can be full or partial. KnowledgeBase Numbers describe artifacts related to Microsoft products, including technical support. When filtering the KB number, we recommend that you don’t use &quot;KB&quot; when entering the number and use operators such as &quot;like.&quot; If you use &quot;equals,&quot; you must enter the information exactly or you get no results. Some numbers start with &quot;KB&quot; and some do not. When using &quot;equals,&quot; you must know whether to use &quot;KB&quot; with the number or not. Note: Multiple KB numbers can be added to a condition by separating each number with a comma.</td>
</tr>
<tr>
<td>MS Number</td>
<td>Enter the Microsoft ID Number(s) for this filter. Numbers can be full or partial. Microsoft ID Numbers describe vulnerabilities identified and listed by Microsoft. Note: Multiple Microsoft numbers can be added to a condition by separating each number with a comma.</td>
</tr>
<tr>
<td>Open Ports</td>
<td>Filter assets based upon the open ports on a system. Note: When entering multiple ports, use a comma to separate each port number.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Determine which operating systems to include or exclude from the report. Enter the exact name of the operating system, or enter partial information (example: win for Windows). Select a setting to include or exclude the operating system(s); or whether the operating system starts or ends with the partially entered text.</td>
</tr>
<tr>
<td>Protocol Name</td>
<td>Identifies all assets with at least one TCP or UDP port open (based on configuration selected).</td>
</tr>
<tr>
<td>Scan Name</td>
<td>Identifies all scan configurations that map to the scan name, then extracts all IP ranges allowed for that scan configurations, and then finds assets within the allowed IP ranges.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>Filter assets by the URL of a given asset. Select to include or exclude the URL from the report. Enter partial information and select whether the selection starts or ends with the partial information.</td>
</tr>
<tr>
<td>Vulnerability Name</td>
<td>Enter a vulnerability name, and set whether to include or exclude this name from the report.</td>
</tr>
<tr>
<td>Vulnerability Severity</td>
<td>Select the vulnerability severity level(s), and set whether to include or exclude the severity level from the report.</td>
</tr>
<tr>
<td>Vulnerability (Vuln Set)</td>
<td>Filter assets based on vulnerabilities found on the asset that are part of a vulnerability set.</td>
</tr>
<tr>
<td>Web Asset</td>
<td>Filter assets by those that have at least one web asset associated with it, or have no web assets associated with it.</td>
</tr>
</tbody>
</table>

### Browse for asset tags in a scan configuration

In a scan configuration, administrators can browse for assets based on asset group or asset tag.

When browsing by an asset tag, the tags appear in a folder tree.

This task describes only the new browse feature related to asset tagging. For information and tasks about the scan configuration process, see the product documentation or online help.

1. In the enterprise manager, select **Scans | Edit Scans**.
2. Create a new scan or edit an existing scan.
3. On the **Targets** tab, click **Browse**.
4. From the **Asset Source** list, select **Asset Tag Set**.
5. Click the name of your organization or workgroup to expand it and display the list of available asset tags.
6. Click the **Toggle Tree** icon, then click the name of an asset tag to display all assets with that tag.
7. Select assets to include or exclude from the scan configuration. Or you can right-click the asset tag name to include or exclude all of the assets with that tag.

### Search for asset tags in a scan configuration

In a scan configuration, administrators can search for assets based on a search type, like asset tag set, IP address, or operating system.

This task only describes the new search feature related to asset tagging. For information and tasks about the scan configuration process, see the product documentation or online help.
1. In the enterprise manager, select **Scans | Edit Scans**.
2. Create a new scan or edit an existing scan.
3. On the **Targets** tab, click **Search**.
4. From the **Search Type** list, select **Asset Tag Set**.
5. From the drop-down list, select the name of an asset tag.
6. Select any **Search Criticalities** you want applied to your search, then click **Search**.
7. Select assets to either include or exclude from the scan configuration.

### Search for assets in asset management

Administrators can search for assets using asset tags, then assign other properties to those assets (like criticality level or owner).

Static asset tags must be applied before the tags can be used in an asset search.

**Note:** Asset tags are not applied to web application assets. Search results based on an asset tag might differ from other search types because the asset tag search results do not include web application assets.

1. In the enterprise manager, select **Manage | Assets**, then click **Search**.
2. Select **Simple Search** or **Advanced Search**.
3. From the drop-down list, select **Asset Tag Set**.
4. Select an asset tag from the list.
5. Select the other criteria for this search.
6. Click **Submit**.
7. To apply properties (like criticality level or owner), you can select a single asset, select multiple assets (using the Ctrl or Alt key), or click **With all search results** (bulk assign).

### Add asset tags to a custom report template

In a custom report template, administrators can add a condition to the asset filter to include or exclude assets based on a tag.

A suffix on the tag name indicates the condition:

- (a) – Dynamic asset tag set to *automatic*
- (m) – Dynamic asset tag set to *manual*
- No suffix – Static asset tag

This task describes adding an asset tag set to a custom report template. For information and tasks about the custom report template process, see the product documentation or online help.

1. In the enterprise manager, select **Reports | Generate Custom Reports**.
2. Create a new custom report template or edit an existing template.
3. On the **Asset Filter** tab, add a condition, then select **Asset Tag Set**.
4. Select **contains** or **does not contain**, then select the asset tag you want to include or exclude.
5. Click **Set Condition**.
6. Continue creating or modifying the template, then click **Save**.
Working with McAfee Vulnerability Manager Scans

When configuring scans, you can use scan templates and scan configurations created by McAfee Vulnerability Manager, or you can create your own.

Scan Status page

The Scan Status page shows the status of all the scans the user has access to. This list shows the pending and active scans so that you can monitor their status. You must have view access to a scan for it to appear on this list.

For this release, the scan status messages provide an accurate status of your scans. Scan details are now available for each scan. The scan details show an ongoing status of the scan while it is running, including discovery details, assessment details, and error messages.

Note: After upgrading from McAfee Vulnerability Manager 7.0.2, or earlier, only completed scans, canceled scans, scans that ended due to an error, and scans that ended due to a license violation display scan detail information. Scans that were in queue, starting, running, or pending during the upgrade do not display scan detail information until the scan successfully completes.

Scan status descriptions

On the scan status page, the Status column displays more messages to provide a more accurate status of your scans.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Awaiting Resources</td>
<td>The scan engine resources are being used by other scans. The scan is put in a paused state. When scan engine resource become available, the scan resumes. If the scan engine is paused, this scan remains in this state until the engine is available.</td>
</tr>
<tr>
<td>Cancel Pending</td>
<td>The scan process is being canceled. A cancel command is sent to the scan engine. All incomplete batches are canceled. If the scan engine is in the process of transferring batch results, the scan engine completes that task and then cancel the scan.</td>
</tr>
<tr>
<td>Canceled</td>
<td>The scan is canceled.</td>
</tr>
<tr>
<td>Complete</td>
<td>The discovery, assessment, and post processing completed.</td>
</tr>
<tr>
<td>Error</td>
<td>The scan ended in an error and did not finish.</td>
</tr>
</tbody>
</table>
### Status Descriptions

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finishing</td>
<td>The scan is in post-processing, like calculating the Foundscore.</td>
</tr>
<tr>
<td>In Queue</td>
<td>The product is preparing the scan based on the scan configuration. The scan launch command is in the command queue; the scan engine has not received the command. The scan details are not available because the scan hasn’t started. You cannot pause or cancel a scan in the In Queue state.</td>
</tr>
<tr>
<td>Offline</td>
<td>The scan engine is either offline or unavailable.</td>
</tr>
<tr>
<td>Pause Pending</td>
<td>The scan process is being paused.</td>
</tr>
<tr>
<td>Paused</td>
<td>The scan is paused.</td>
</tr>
<tr>
<td>Engine Paused</td>
<td>The scan engine was paused.</td>
</tr>
<tr>
<td>Pending</td>
<td>The scan engine has received the command but has not responded with a success or failure.</td>
</tr>
<tr>
<td>Resume Pending</td>
<td>The scan process is starting from the paused state.</td>
</tr>
<tr>
<td>Running</td>
<td>The scan is running. See the scan details for more detailed information about the scan.</td>
</tr>
<tr>
<td>Starting</td>
<td>The scan engine has received the command and successfully responded. The scan engine is starting the scan, which includes resolving host names, sending information to the scan engine, and finding hosts. You cannot pause or cancel a scan in the Starting state.</td>
</tr>
</tbody>
</table>

### Scan detail descriptions

The scan details show the progress of different processing during a scan. The following information describes the different scan detail information.

Some scan types perform assessment but do not scan for vulnerabilities. These scans show less information in the Discovery and Assessment sections. The Vulnerabilities by Risk pie chart is grayed out. These scan types include the Baseline Policy scan, XCCDF Benchmark scan, and McAfee Policy Auditor Data Collection scan.

To understand the scanning process, see *How the product scans hosts* (page 56).
Scan detail description

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Timeline</td>
<td>Shows the progress of the current scan using a green bar. The bar is orange if the actual scan time is significantly longer than the estimated duration. The scan timeline does not appear the first time you run a scan. The scan timeline appears after the first successful completion of the scan.</td>
</tr>
<tr>
<td>Estimated Duration</td>
<td>Shows the estimated time the scan should take to complete, based on the completion history of the scan. The estimated duration does not appear the first time you run a scan. The estimated duration only appears after the first successful completion of the scan. The estimated duration works best when the scan configuration remains consistent (like the number of hosts being scanned and the vulnerabilities). Modifying Previous Duration Shows the duration of the last time the scan completed. Scans that were canceled or failed are not taken into consideration.</td>
</tr>
<tr>
<td>Previous Duration</td>
<td></td>
</tr>
<tr>
<td>Start</td>
<td>Displays the date and time the scan started.</td>
</tr>
<tr>
<td>End</td>
<td>Displays the date and time the scan ended.</td>
</tr>
<tr>
<td>Duration</td>
<td>Displays the amount of time (hh:mm:ss) between when a scan started and when it ended. The scan start time is obtained from the scan engine and the end time is obtained from the API server. If the scan engine and the API server are on different servers and the server clocks are not synchronized, you get an inaccurate scan time.</td>
</tr>
<tr>
<td>Engine</td>
<td>Displays the scan engine used during the scan.</td>
</tr>
</tbody>
</table>
| Discovery           | Shows the progress and details about the discovery portion of the scan.  
  - **Hosts found** – Number of hosts found compared to the number of possible hosts. Possible hosts include all IP addresses in an IP range, even if the IP address is not being used by a host.  
  - **Network saturation** – Percentage of discovered hosts compared to the number of potential hosts.  
  - **Services found** – Total number of services found on all hosts discovered by the scan.  
  - **Average services per host** – Total number of services divided by the total number of discovered hosts.  
  - **Discovery batches completed** – Number of discovery batches completed compared to the total number of discovery batches.  
  - **Successful login(s)** – Number of hosts the scan could successfully log on to based on the credentials or credential set included in the scan configuration. |
<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovered Operating Systems</td>
<td>Shows the five operating systems with the highest number of discovered hosts and the number of hosts running other operating systems (<em>Other Operating Systems</em>). Hovering over a pie slice displays the number of hosts found with that operating system. Clicking on the pie chart displays a list of all operating systems and the number of hosts in each.</td>
</tr>
</tbody>
</table>
| Assessment                     | Shows the progress and details about the assessment portion of the scan.  
• **Hosts assessed** – Number of hosts assessed compared to the number of hosts discovered.  
• **Hosts not assessed** – Number of hosts not assessed by the scan. This includes hosts that were partially assessed, like an assessment timing out when the maximum amount of time allowed to scan a single host is reached.  
• **Vulnerabilities found** – Total number of vulnerabilities found on all hosts assessed by the scan.  
• **Average vulns per host** – Total number of vulnerabilities divided by the total number of assessed hosts.  
• **Assessment batches completed** – Number of assessment batches completed compared to the total number of assessment batches. |
| Vulnerabilities by Risk        | Shows the high, medium, low, and informational vulnerabilities found as a pie chart. Hovering over a section of the pie chart shows the number of vulnerabilities discovered for that risk level. |
| Post Processing                | Shows the progress of the post processing for the scan. Post processing begins after assessment is complete. Post processing includes updating asset data, computing data (like FoundScore), and adding the report to the queue for generating the scan report. |
| Logs                           | Shows the last five log messages for the scan. The logs are updated at regular intervals.  
This information comes from the scan engine. If the scan controller is on the same server as the scan engine, the scan controller log messages should display.  
These messages are provided to show the scan is still active. Some scan processes, like batch processing, can take a long time to complete, and during that time, the scan might appear to be stuck. The log messages show if the scan is still active by updating every 10 seconds. If the messages do not change for a long time, the scan might be stuck. |
Working with McAfee Vulnerability Manager Scans
Scan Status page

<table>
<thead>
<tr>
<th>Detail</th>
<th>Description</th>
</tr>
</thead>
</table>
| Errors | If one or more errors occur during a scan, an error link is available on the Scan Details page. Click the errors link to view a list of errors.  
This information comes from the scan engine. If the scan controller is on the same server as the scan engine, the scan controller error links should display.  
There are scan events that are logged as errors that do not negatively impact the scan. McAfee recommends only viewing the error messages if your scan fails, with the help of technical support.  
For recovered scans, the error count might be inaccurate, depending on how much work must be redone to recover the scan. Scan recovery occurs when a scan engine is restarted during a scan.  
**Note:** Organization administrators, workgroup administrators, and the global administrator can view scan errors. |

**How the product scans a host**
To understand the scan status updates and the scan details, you should understand how the scanning process works.

The following is a summary of the McAfee Vulnerability Manager scanning process.

1. When the scan process starts:
   a. The scan launch command is in the command queue (*In Queue*).
   b. The scan engine receives the command (*Pending*).
   c. The scan engine responds successfully (*Starting*).
   d. The scan engine starts the scan process (*Running*).

2. During the discovery process:
   a. The product takes the number of assets (host names) and IP addresses, and divides these into subscans.
   b. The product takes the number of assets and IP addresses in a subscan, and creates batches.
   c. The product runs the discovery process on each batch, trying to find active hosts, along with the operating system and any services running on each host. Data is sent to the database and the scan details are updated after each batch completes.

3. During the assessment process:
   a. The product takes all active hosts and divides them into subscans.
   b. The product takes the number of hosts in a subscan and creates batches.
   c. The product runs the vulnerability scripts against each host. Data is sent to the database and the scan details are updated after each batch completes.

4. During post processing, the FoundScore and statistics data are computed, the threat index is updated, and the report command is sent to the queue.

Subscans and batches help the scan process by separating the IP addresses into smaller groups and allow the product to process them in parallel, or use multiple threads.

The number of subscans is simply the maximum number of groups the product can divide IP addresses into. The default is five. If there are 5,000 IP addresses, then the product divides them into five subscans of 1,000 IP addresses each.
A batch is a small group of IP addresses (from a subscan) that the product scans and processes data for.

- For a discovery scan, the default batch size is 1024 IP addresses. With 1,000 IP addresses per subscan, the product creates one batch. The default batch size for a Discovery scan is larger than a Vulnerability scan because the Discovery scan is only looking for active hosts in the batch. If you change the batch size under the Optimize settings, the Discovery scan uses those settings.
- For a vulnerability scan, the default batch size is 64 IP addresses. So with 1,000 IP addresses, the product creates about 16 batches. The default batch size for a Vulnerability scan is smaller than a Discovery scan because the Vulnerability scan is running scripts against each active host in the batch. If you change the batch size under the Optimize settings, the Vulnerability scan only allows 64 IP addresses or less. Example: If you set the batch size to 128, the Vulnerability scan still creates batches of 64 IP addresses (or less).

Vulnerability scripts are not included in a batch. Instead, vulnerability scripts are run against a batch. The scan engine goes through all of the scripts against a batch before any of that data is sent to the database.

The scan status and scan details are not updated until the data processing for the batch is complete. This can cause the scan progress to stay at a percentage for a while and then suddenly jump to a new percentage. This is especially noticeable with small scans that have only a few batches.

---

**How scan configuration settings work**

McAfee Vulnerability Manager provides some preconfigured scan templates and scan configurations to assist most users with their scanning needs.

You can also use the scan templates and scan configurations as a starting point, modify the template or configuration to suit your needs, and save it as your own.

The product provides the following types of scan templates:

- **Vulnerability Template** – Scan templates that include HIPAA and PCI.
- **Compliance Template** – Scan templates that include the Baseline Policy and FDCC.
- **XCCDF Template** – Scan templates that include the XCCDF Benchmark scan.
- **Web Template** – Scan templates that include OWASP Top 10 and PCI DSS compliance.

**Create a scan configuration**

You can use a preconfigured scan template or create a custom scan template when configuring a scan.

1. Select **Scans | New Scan**.
2. On the **Scan Details** page, select the type of scan you want to create, then click **Next**.
   - **Use McAfee Vulnerability Manager's default settings** – Create a scan based on the default settings.
   - **Use a McAfee Vulnerability Manager template** – Create a scan based on a template. Select the template you want to use.
   - **Use an existing scan** – Create a scan based on an existing scan. Select the scan you want to use.
3. On the **Targets** tab, type the **Scan Name**. Typing a **Description** and selecting a **Scan Type** are optional.
4. Specify the IP addresses to scan by, then click **Next**.
   - Typing IP addresses
Working with McAfee Vulnerability Manager Scans
How scan configuration settings work

- Browsing through a list of assets
- Searching for specific assets
- URL or host name

**Note:** Binding an asset to an IP address is done at scan time instead of scan configuration, whether you entered a host name, IP address, or URL. Scheduled scans rebind an asset to an IP address each time the scan is run. Any asset that resolves to an IP address outside your valid IP range is not scanned.

5 Click the icon on the left side of the page to change the settings, then click **Next**.
   - **Hosts** – Specify options for ICMP, UDP, and TCP scanning Also select/deselect the Asset Tagging option.
   - **Services** – Specify the services you want discovered on your network
   - **Credentials** – Create and manage credentials used to access systems on your network
   - **Vuln Selection** – Specify the vulnerabilities you want checked under the General, Windows, Wireless, and Shell categories
   - **Optimize** – Change settings to optimize the performance of the product
   - **Web App Config** – Specify the entry paths, exclude paths, exclude parameters, and port pairs for web application scans

6 Specify whether you want to create remediation tickets for this scan when it has completed running. Deselect the checkbox if you do not want remediation tickets created.

7 Select the **FoundScore Type** you want used for this scan (**Internal** or **External**). This setting defines the set of calculations used to determine the FoundScore value.

8 Select the format in which you want reports created.

9 Select the sections you want to include in the report, then click **Next**.

10 Select if you want this scan activated or deactivated. If you decide to activate this scan, and set the type to **Immediate** the scan starts after you save it. Deactivated scans are saved but are not run automatically (you can run them manually by clicking Activate in the Edit Scans page).

11 Select the scan engine and specify the network interface.

**Note:** If the Select Engine displays **AutoSelect**, the Global Administrator or Root Organization Administrator has enabled automatic scan engine selection. The scan automatically selects a scan engine based upon the IP addresses selected for this scan.

12 Schedule the scan to run immediately, at a specific date and time, or on a recurring schedule.

13 If you want to use a scan window, so that the scan runs during specific hours or on specific days, select the checkbox and enter the window details.

14 Select a time zone to coordinate the scan start time.
   - **Use Engine Time** – The scan start time is based on the time zone of the scan engine.
   - **Use Local Time** – The scan start time is based on the time zone you select (UTC time).

**Note:** UTC time is constant. If the selected timezone alters the time (like daylight savings time), the start time for a recurring scan changes.

15 Save the scan.
   - **Save and Scan Now** – **Active** and **Immediate** are selected. This saves the scan configuration and starts the scan.
   - **Schedule Scan** – **Active** and **One Time** or a recurring schedule are selected. This saves the scan configuration and the scan starts at the scheduled date and time.
   - **Save** – **Inactive** is selected. This saves the scan configuration without starting the scan.
Creating credential sets

You can manage your scan credentials as a set and select a credential set to be used in a scan configuration. If you must change your credentials, you only need to change the appropriate credential set instead of every single scan using those credentials.

By default, credential sets are available to the credential set creator (organization administrator or workgroup administrator). A credential set made Public allows workgroup administrators below the credential set creator to view and use the selected credential set, but they cannot edit or delete the set. McAfee Vulnerability Manager users (non-administrators) can only add credentials to scan configurations, they cannot view or use credentials sets (even Public credential sets). In a scan configuration, if a credential is added that matches the user name, domain, and password to a credential in the selected credential set, the credentials are merged before scanning.

Administrators above the creator of the credential set can view, use, edit, and delete the credential set.

Create a credential set

1. Select Components | Credential Sets.
2. Click Create New.
3. On the Start tab, give the credential set a unique name and an optional description. The credential set name must be unique compared to other credential sets in the organization.
4. Select Public if this credential set can be used by workgroup administrators. Making a credential set Public allows workgroup administrators under the credential set creator to view and use the selected credential set.

Note: If a public credential set is used in a scan configuration and the credential set is modified to no longer be public, this does not automatically remove the credential set from the scan configuration. The credential set must be manually removed from the scan configuration.

5. Click Next.
6. Select a credential type to add.
7. Type the domain, workgroup, host, default, server, or URL.
8. Type the credential information.
9. Click Add/Update to add the credential, then click Save.

Modify a credential set

NOTE: When a scan is using a credential set, you can edit the credential set while the scan is running. Changes made to the credential set take affect the next time the scan starts. Examples: the next time a scan is scheduled to start, manually activating a scan, cancelling and re-activating a scan. Pausing and resuming a scan does not apply the changes to the credential set.

1. Click View/Edit.
2. On the Start tab, edit the name and description of the credential set.
3. On the Credentials tab, add, edit, or remove credentials.
4. Click Save.
5. To duplicate a credential set, click Save As and give the credential set a unique name.
Check which scans are using a credential set

1. Click the **Yes** link in the **In Use** column. A table appears with a list of scans currently using the selected credential set.
   - **Scan Name** – The name of the scan using the credential set.
   - **Description** – The description of the scan.

2. Click **Back** to return to the previous page.

Delete a credential set

**NOTE**: You cannot delete a credential set that is being used by a scan configuration. To delete a credential set that is In Use, you must first remove the credential set from all scan configurations.

1. Click **Delete** for the credential set.
   - A message prompts you to confirm the action.

2. Click **Yes** to delete the credential set.

Credential set details

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the credential set.</td>
</tr>
<tr>
<td>Description</td>
<td>The description of the credential set.</td>
</tr>
</tbody>
</table>
| In Use    | *Yes* – This credential set is being used by one or more scan configurations. Click the **Yes** link to view which scan configurations are currently using this credential set.  
|           | *No* – This credential set is not being used by any scan configurations.        |
| Create New | Goes to the set up page so you can create a new credential set.             |

**Perform SSH key collection**

When a scan engine cannot authenticate to an untrusted shell target, the scan fails and an error message appears in the Application Status.

The product does allow you to trust unknown remote-shell targets, but this is not recommended for security reasons. If you trust unknown shell targets, you could provide root user authentication to the wrong person.
Working with McAfee Vulnerability Manager Scans
How scan templates work

1. Create a discovery scan and add shell targets.
2. On the Settings tab, select Optimize.
3. Select Perform SSH Key Collection.
4. Complete the scan configuration and run the scan.
5. After the scan completes, select Manage | Assets.
6. Select the shell assets you want to mark as trusted systems.
7. Right-click and select Mark as Trusted. If you need to remove an asset from the trusted list, right-click and select Remove Trust.
8. Create a vulnerability scan, add your trusted shell targets, and include shell credentials.

How scan templates work

McAfee Vulnerability Manager provides scan templates to cover most user needs. The product comes with default templates that can be used to create your own scans. These templates have been carefully designed, based on the best-practices developed by McAfee’s Sales Engineers. The settings are determined by the size of the network and by the type of scan.

You can use the provided scan templates as a guide. Once you have created a scan based on a template, you can go in and change the settings, refining them to match your network configuration as needed. Refer to this guide for more information on each setting.

For the purposes of describing network sizes, this guide uses the following size definitions:

- **Small Network** – Up to 10 Class C networks (2560 potentially live hosts)
- **Medium Networks** – Multiple Class C networks up to a Class B network (65536 potentially live hosts)
- **Large Networks** – Multiple Class B networks up to a Class A network (16.7 million potentially live hosts)

Create a scan with a vulnerability scan template

When creating a new scan, you can select a vulnerability template, compliance template, or a XCCDF template to create your scan.

1. Select Scans | New scan.
2. On the Scan details page, select the type of scan you want to create, then click Next.
   - To create a scan based on the default settings, select Use McAfee Vulnerability Manager’s default settings.
   - To create a scan based on a template, select Use a McAfee Vulnerability Manager template, select the template you want to use.
   - To create a scan based on an existing scan, select Use an existing scan, select the scan you want to use.
3. On the Targets tab, type the Scan Name. Typing a Description and selecting a Scan Type are optional.
4. Specify the assets to be scanned, then click Next.
   - On the Targets tab, type the asset IP address, URL, or host name.
   - On the Browse tab, select a source and then select the assets.
   - On the Search tab, specify the search criteria to find the assets.
Working with McAfee Vulnerability Manager Scans
How to use custom scan templates

Note: The product now performs late binding. Asset binding is done at scan time instead of scan configuration. Scheduled scans rebind assets to IP addresses each time the scan is run.

5 Click the icon on the left side of the page to change the settings, then click Next.
- Hosts – Specify options for ICMP, UDP, and TCP scanning Also select/deselect the Asset Tagging option.
- Services – Specify the services you want discovered on your network
- Credentials – Create and manage credentials used to access systems on your network
- Vuln Selection – Specify the vulnerabilities you want to scan for under the General, Windows, Wireless, Web, and Shell categories
- Optimize – Change settings to optimize the performance of the product
- Web App Config – Specify the entry paths, exclude paths, exclude parameters, and port pairs for a web application scan

6 Specify if you want to create remediation tickets for this scan when it has completed running. Deselect the checkbox if you do not want remediation tickets created.

7 Select the FoundScore Type you want used for this scan (Internal or External). This setting defines the set of calculations used to determine the FoundScore value.

8 Select the format in which you want reports created, then click Next.

9 Select Active to enable the scan. If you decide to activate this scan and set the Schedule Type to immediate, the scan starts right after you save it. Inactive scans are saved but are not run automatically (you can run them manually by clicking Activate on the scan configuration page).

10 Select the scan engine.

Note: If the Select Engine displays AutoSelect, the Global Administrator or Root Organization Administrator has enabled automatic scan engine selection. The scan automatically selects a scan engine based upon the organization or workgroup selected for this scan.

11 Select a time zone to coordinate the scan start time.
- Use Engine Time – The scan start time is based on the time zone of the scan engine.
- Use Local Time – The scan start time is based on the time zone you select (UTC time).

Note: UTC time is constant. If the selected timezone alters the time (like daylight savings time), the start time for a recurring scan changes.

12 Save the scan.
- Save and Scan Now – Active and Immediate are selected. This saves the scan configuration and starts the scan.
- Schedule Scan – Active and One Time or a recurring schedule are selected. This saves the scan configuration and the scan starts at the scheduled date and time.
- Save – Inactive is selected. This saves the scan configuration without starting the scan.

How to use custom scan templates

You can create a custom scan template based on a McAfee Vulnerability Manager scan template, or create a new scan template.

When you create a new scan template, you can select the hosts, services, vulnerability selections, web module, and optimization settings.

After you create a custom scan template, it appears in the Use a Common template list when you create a new scan (page 57).
Create a custom scan template

1. Log on as the Global Administrator.
2. Select **Scans** | **New template**.
3. Select a base setting for your scan, then click **Next**.
   - **Use McAfee Vulnerability Manager's default settings** – This is the default scan template. You can base a new scan template on the default template and change the settings as desired to customize it.
   - **Use a McAfee Vulnerability Manager template** – The available templates appear on the bottom half of the page. Select a template.
   - **Start a new template** – Start with a blank scan template and select your template options (hosts, services, vulnerability selection).
4. On the **Targets** tab, type the **Scan Name** and **Description**. **Targets** and **Scan Scheduling** are not available when creating a scan template. These settings are available when creating a scan configuration.
5. Click **Next** or click the **Settings** tab.
6. Select options for **Hosts**, **Services**, **Vuln Selection**, and **Optimize**. When creating scan templates, **Credentials** and **Web App Config** settings are not available.
7. Click **Next** or click the **Reports** tab.
8. Select remediation options and FoundScore Type.
9. Select report options and sections for this template, then click **Save**.

How vulnerability sets work

Create a vulnerability set and add the vulnerabilities that are important to your organization.

You can add a vulnerability set to a scan configuration, custom report, or asset tag, modify the vulnerability set, and have those updated vulnerability selections applied to all scan configurations, custom reports, and asset tags using the vulnerability set. You can add one vulnerability set to a scan configuration or custom report template.

When adding vulnerabilities to a set, you can select the vulnerabilities from a tree structure, or you can create rules for selecting vulnerabilities.

Only organization and workgroup administrators can create vulnerability sets. Administrators above the vulnerability set creator can modify, duplicate, or delete the vulnerability set. Administrators below the set creator can only view or duplicate the vulnerability set.

- **Creating a vulnerability set using the vuln tree** (page 63) – Allows you to select vulnerabilities from a list of vulnerabilities. You can view vulnerabilities by type or search for them.
- **Creating a vulnerability set using rules** (page 65) – Allows you to select criteria in the rule editor for selecting vulnerabilities. You can preview the rules to see which vulnerabilities are selected based on your rules.

Create a Tree Based vulnerability set

Select vulnerabilities from the vulnerability tree when you want to include specific vulnerabilities in your scan configurations, custom reports, and asset tags.

A vulnerability tree based vulnerability set works the same as the vulnerability tree in a scan configuration. All vulnerability categories are set to not use new vulnerability checks each time the
scan is run. You can modify this using advanced settings so that new vulnerability checks are used each time the scan is run.

1. In the enterprise manager, select **Components | Vuln Sets**.
2. Click **Create New**.
3. Type a name and an optional description for the vulnerability set.
4. Select **Tree Based** for the Type, then click **Next**.
5. Select vulnerabilities from the tree. You can select which vulnerability modules to enable or disable (General, Windows, Wireless, Shell, and Web App). You can also use the Display By list or use Search to find vulnerabilities.

   **Note:** The vulnerability modules only work when displaying by Category (not by Risk Level, CVE, or MS Number).

6. Click **Advanced**, then select **Run New Checks** for any vulnerabilities you want the scan configuration to check for updates every time the scan is run.
7. Click **Save**.

### Vulnerability tree options

The following table describes the options available for use in the vulnerability tree.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modules enabled</td>
<td>Changes which modules are available in the Vulnerability Set.</td>
</tr>
<tr>
<td>Display by</td>
<td>Changes the way the vulnerability checks are displayed on this page:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Category</strong> – Displays the vulnerability checks in categories. Vulnerability check categories fall into two important categories: Intrusive – These checks are likely to interfere with the host’s normal operating behavior. Some intrusive checks can cause a denial-of-service condition or require that the host be restarted. If you enable Intrusive checks, monitor the devices both during and after the scan to ensure they are performing as anticipated. Non-Intrusive – These checks do not affect the host being scanned.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MS Number</strong> – Sorts and categorizes the vulnerability checks according to the Microsoft Security Bulletin numbers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Risk Level</strong> – Sorts and displays the vulnerability checks according to their risk level: Informational, Low, Medium, and High.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CVE</strong> – Sorts and categorizes the vulnerability checks according to their CVE numbers.</td>
</tr>
</tbody>
</table>

**Warning:** When displaying vulnerability checks by CVE Number or Risk Rating, the intrusive checks and non-intrusive checks are combined. Selecting the entire CVE Number or Risk Rating categories results in selecting a mixture of intrusive and non-intrusive checks.
Search by Select the data you want to search by:

- **Name** – Search through vulnerability check names.
- **CVE Number** – Search for a specific CVE number.
- **MS Number** – Search for an MS number.
- **FaultlineID** – Search for a FaultlineID.
- **Risk Level** – Select a risk level: High, Medium, Low, or Informational.

Enter the criteria you want to search, based on your **Search by** selection.

---

**Create a Rule Based vulnerability set**

Create rules when you want to include all vulnerabilities that meet a set of criteria. Vulnerability sets can be used in scan configurations, custom report templates, and asset tags.

The rules are evaluated when:

- A scan is run or a custom report is generated.
- Performing a simple or advanced asset tag search.
- Browsing or searching for targets using an asset tag when creating a scan configuration.

New checks are added automatically if they match the rules defined in a rule-based vulnerability set when the scan configuration using this set runs.

**Note:** In Microsoft Internet Explorer, the Internet security settings for Internet and Local Internet must be set to default for the rule pop-up window to display.

1. In the enterprise manager, select **Components | Vuln Sets**.
2. Click **Create New**.
3. Type a name and an optional description for the vulnerability set.
4. Select **Rule Based** for the Type.
5. Click the **Rules** tab. The rule "Intrusive equals No" is added by default, which means only non-intrusive vulnerability checks are added to the scan configuration.
6. Select one of these options:
   - **Add Condition** – Add a condition at the current level in the hierarchy.
   - **Add Nested Condition** – Create a new condition on a new child level in the hierarchy. Nested conditions share the same operator.
7. Select a condition type from the list.
8. Select criteria for the condition.
9. Click **Set Condition**.
10. Click **Preview Rules** to view the vulnerability tree, with the vulnerabilities selected based on the conditions of your rules.
11. Click **Save**.
Vulnerability rule options

The following table describes the conditions available for use in the vulnerability set rule editor.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category</td>
<td>Select an operator (equals or does not equal), then type the category name. As you type the name, a list appears. Select a category from the list or type out the full category name.</td>
</tr>
<tr>
<td>CVE Number</td>
<td>Select an operator (contains or does not contain), then type a CVE string. This includes or excludes the vulnerabilities associated with the CVE string.</td>
</tr>
<tr>
<td>CVSS Metrics</td>
<td>Select a CVSS metric, operator (contains or does not contain), and other rule options.</td>
</tr>
<tr>
<td>CWE</td>
<td>Type a CWE and select to include or exclude the vulnerabilities associated with the CWE.</td>
</tr>
<tr>
<td>Intrusive</td>
<td>Select to include intrusive or non-intrusive vulnerability checks.</td>
</tr>
<tr>
<td>Module</td>
<td>Select to include or exclude vulnerabilities based on a module (General Vulnerability, Windows Host, Wireless, Shell, or Web).</td>
</tr>
<tr>
<td>MS Number</td>
<td>Type an MS number and select to include or exclude vulnerabilities associated with the MS number.</td>
</tr>
<tr>
<td>Patch Availability</td>
<td>Sorts and categorizes the vulnerability checks based on the availability of known patches for vulnerabilities.</td>
</tr>
<tr>
<td>Risk</td>
<td>Select a risk level and condition to include vulnerabilities that match the condition.</td>
</tr>
<tr>
<td>Specific Vulnerability</td>
<td>Type a vulnerability and select to include or exclude the vulnerability.</td>
</tr>
<tr>
<td>Vulnerability Name</td>
<td>Enter a vulnerability name, and set whether to include or exclude this name.</td>
</tr>
<tr>
<td>Vulnerability Severity</td>
<td>Select the vulnerability severity level(s), and set whether to include or exclude the severity level.</td>
</tr>
</tbody>
</table>

Modify a vulnerability set

You can add or remove vulnerabilities from a set, and those changes affect any scan configurations, custom report templates, and asset tags using it. This allows you to quickly modify the vulnerabilities you are scanning and reporting on.

You can also change the type, like from tree based to rule based. This allows you to change the vulnerability set for multiple scan configurations and custom report templates in one location.

Note: Changing the vulnerability set type erases any vuln tree selections or rules created.
Working with McAfee Vulnerability Manager Scans
How vulnerability sets work

1. In the enterprise manager, select **Components | Vuln Sets**.
2. Click **View/Edit**.
3. Select the **Vuln Tree** tab if the set is tree based. Select the **Rules** tab if the set is rules based.
4. Add or remove vulnerabilities (tree based) or rules (rules based) from the set.
5. Click **Save**.

**Duplicate a vulnerability set**

Duplicating a vulnerability set allows you to use an existing set as a starting point, and then modify the set as needed.

1. In the enterprise manager, select **Components | Vuln Sets**.
2. Click **View/Edit**.
3. Click **Save As**. A message appears.
4. Click **OK**. A duplicate set is created and Copy Of is added to the name.
5. Type a new name and an optional description for the vulnerability set.
6. Depending on the type, add vulnerabilities using the Vuln Tree or add rules using the rule editor.
7. Click **Save**.

**Delete a vulnerability set**

You can delete vulnerability sets that are no longer needed. Before you can delete a vulnerability set, you must remove it from all scan configurations, custom report templates, and asset tags.

1. In the enterprise manager, select **Components | Vuln Sets**.
2. Click **Delete**. A confirmation message appears.
3. Click **OK**.

**Add a vulnerability set to a scan configuration**

After creating a vulnerability set, you can add it to your scan configurations.

1. Create a new scan configuration, or edit an existing one.
2. On the **Settings** tab, select **Vuln Set**, then select a vulnerability set. You can type part of the vulnerability set name and the first 20 matching sets appear in the list.
3. Click **Preview** to view the vulnerabilities included in the set.
4. Update the rest of the scan configuration, then click **Save**.

**Note**: A set might contain vulnerability checks that require credentialed access to the system being scanned. If necessary, include credentials on the Settings page of a scan configuration.

**Add a vulnerability set to a custom report**

When creating a custom report template, you can include a vulnerability set on the Asset Filter tab and the Sections tab.

Adding a vulnerability set on the Asset Filter tab includes the assets that are vulnerable to one or more of the vulnerabilities specified in the set. Adding a vulnerability set on the Sections tab includes only vulnerabilities from the set in the custom report.
If you want to change the vulnerability set being used, edit the custom report template and select a different vulnerability set.

1. On the Asset Filter tab for a custom report template, click Add Condition or Add Nested Condition.
2. Select Vulnerability (Vuln Set) from the list. The only operator available is contained in.
3. Type the name of the vulnerability set. As you type, a list of sets appears. You can type the full name of the set or select one from the list.

   **Note:** The vulnerability set list displays the first 20 matching entries.

4. Click Set Condition.
5. On the Sections tab, select Vulnerability Assessment.
6. Click Select Vulnerabilities.
7. Select Vuln Set, then select a vulnerability set.
8. Click OK.
9. Update the rest of the custom report template, then click Save.

### Check for vulnerability sets in use

Before a vulnerability set can be deleted, the set must be removed from any scan configuration, custom report template, or asset tag using it.

**Note:** If a vulnerability set is in use, the Delete button is not available.

1. In the enterprise manager, select Components | Vuln Sets.
2. If the vulnerability set is being used, click Yes under In Use.
3. View the list of scan configurations, custom report templates, and asset tags using the vulnerability set.

**Note:** This list displays only scan configurations and custom report templates that you have access to. A warning message appears if there are scan configurations or custom report templates using this set that you do not have access to.

### McAfee vulnerability sets

McAfee vulnerability sets provide some predefined vulnerability sets based on popular compliance standards. The vulnerability set gets the latest information from the compliance standard each time the scan is run.

The compliance standards include the latest Microsoft patches. These predefined vulnerability sets are read-only and cannot be modified. You can, however, create a copy of the read-only vulnerability set and modify it to meet your needs.

**Note:** If you use data synchronization to import data from one product database to another with McAfee vulnerability sets referenced in scan configurations, see Using McAfee vulnerability sets in synchronized data (page 70).
Add a McAfee vulnerability set to a scan configuration

Using McAfee vulnerability sets allows scans to search for the latest compliance information without having to update the scan configurations.

This task describes adding a McAfee vulnerability set to a scan configuration. For information and tasks about the scan configuration process, see the product documentation or online help.

1. In the enterprise manager, select **Scans | Edit Scans**.
2. Create a new scan or edit an existing scan.
3. On the Settings tab, select **Vuln Selection**.
4. Select a McAfee vulnerability set from the drop-down list. These begin with _McAfee_.
5. Continue creating or modifying the scan configuration, then click **Save**.

Add a McAfee vulnerability set to a custom report template

Assets with vulnerabilities that match the vulnerability set are added to the report when it is generated.

This task describes adding a McAfee vulnerability set to a custom report template. For information and tasks about the custom report template process, see the product documentation or online help.

1. In the enterprise manager, select **Reports | Generate Custom Reports**.
2. Create a new custom report template or edit an existing custom report template.
3. On the Settings tab, select **Vuln Selection** or **Asset Filter**.
4. Select a vulnerability set from the drop-down list.
5. Continue creating or modifying the template, then click **Save**.

Add a McAfee vulnerability set to a scan template

The global administrator can create a scan template and include a McAfee vulnerability set for the Vuln Selection.

This task describes adding a McAfee vulnerability set to an scan template. For information and tasks about the scan template process, see the product documentation or online help.

1. Log on as the global administrator.
2. Select **Scans | New Template**.
3. Select a base setting for your scan template, then click **Next**.
4. Type a name for the scan template, then click **Next**.
5. Under **Vuln Selection**, select a McAfee vulnerability set from the list.
6. On the Settings and Reports tabs, select your other options, then save the template.

Create a vulnerability set based on a McAfee vulnerability set

McAfee vulnerability sets cannot be edited, but administrators can create a copy and then modify the set as needed.
Working with McAfee Vulnerability Manager Scans

McAfee vulnerability sets

1. In the enterprise manager, select **Components | Vuln Sets**.
2. Select **McAfee Vulnerability Sets**.
3. Click **Save As** for the vulnerability set you want to copy.
4. Type in a new name for the vulnerability set.
5. Modify the vulnerability set as needed.
6. Click **Save**.

**View McAfee vulnerability sets in use**

Administrators can check which McAfee vulnerability sets are being used in a scan configuration, custom report template, or asset tag.

1. In the enterprise manager, select **Components | Vuln Sets**, then click the **McAfee Vulnerability Sets** tab.
2. If the vulnerability set is being used, click **Yes** under **In Use**. View the list of scan configurations and custom report templates using the vulnerability set.

**Note:** This list displays only scan configurations and custom report templates that you have access to. A warning message appears if there are scan configurations or custom report templates using this set that you do not have access to.

**Use McAfee vulnerability sets in synchronized data**

When synchronizing data from one product database into another, McAfee vulnerability sets referenced in imported scan configurations are saved as an editable vulnerability sets with similar settings (at the time of the synchronization).

The imported vulnerability set is editable and has the same name as the McAfee vulnerability set. This does not affect the scan configuration or vulnerability sets in the product instance you imported from.

If you are synchronizing data because the remote McAfee Vulnerability Manager instance is no longer be, and you need to run the imported scan configuration, edit the scan configuration, then select the McAfee vulnerability set instead of the custom vulnerability set.

**Note:** When synchronizing data, both product instances must be on the same version (McAfee Vulnerability Manager 7.0.2 to 7.0.2).

1. After the data synchronization is complete, select **Components | Vuln Sets**.
2. Under Vulnerability Sets, look for sets that begin with **_McAfee_**.
3. Click the **In Use** link to find all scan configurations using the custom vulnerability set.
4. Edit each scan configuration, select **Do not use a vuln set** under Vuln Selections settings, then save the scan configuration.
5. Select **Components | Vuln Sets**.
6. Click **Delete** for the custom vulnerability set you want to delete, then click **OK** to confirm the deletion.
Vulnerability sets based on CVSS scores

Administrators can create a rule-based vulnerability set that is based on CVSS scores.

This topic covers only the addition of CVSS scores for a rule-based vulnerability set. For more information about vulnerability sets, see *Using vulnerability sets* (page 63).

<table>
<thead>
<tr>
<th>Item</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVSS Access Vector</td>
<td>Reflects how the vulnerability is exploited. The more remote an attacker can be to attack a host, the greater the vulnerability score.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Requires local access</strong> – A vulnerability exploitable with only local access. The attacker must have either physical access to the host or a local (shell) account (examples: Firewire/USB DMA attacks, local privilege escalations)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Adjacent network accessible</strong> – A vulnerability exploitable with adjacent network access. The attacker must have access to either the broadcast or collision domain of the vulnerable software (examples: local IP subnet, Bluetooth, local Ethernet segment)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Network accessible</strong> – The vulnerable software is bound to the network stack and the attacker is not required to have local network access or local access (example: RPC buffer overflow)</td>
</tr>
<tr>
<td>CVSS Access Complexity</td>
<td>Measures the complexity of the attack required to exploit the vulnerability once an attacker has gained access to the target system</td>
</tr>
<tr>
<td></td>
<td>• <strong>High</strong> – Specialized conditions exist (i.e. attacker must have elevated privileges or spoof additional systems in addition to the attacking system)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong> – Access conditions are somewhat specialized (example: attacker is limited to a group of systems or users at some level of authorization, possibly untrusted)</td>
</tr>
<tr>
<td></td>
<td>• <strong>Low</strong> – Specialized access conditions do not exist</td>
</tr>
</tbody>
</table>
CVSS Authentication measures the number of times an attacker must authenticate to a target in order to exploit a vulnerability.

- **Requires multiple instances of authentication** – Requires an attacker to authenticate two or more times, even if the same credentials are used each time (example: authenticating to an operating system and then having to provide credentials to access an application on that system)
- **Requires single instance of authentication** – Only one instance of authentication is required to access and exploit the vulnerability.
- **Requires no authentication** – Authentication is not required to access and exploit the vulnerability.

---

CVSS Confidentiality Impact measures the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized users.

- **None** – There is no impact to the confidentiality of the system
- **Partial** – There is considerable information disclosure (access to some system files is possible, but the attacker does not have control over what is obtained)
- **Complete** – Total information disclosure, resulting in all system files being revealed (the attacker is able to read all data on the system)

---

CVSS Integrity Impact measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information.

- **None** – There is no impact to the integrity of the system
- **Partial** – Modification of some system files or information is possible, but the attacker does not have control over what can be modified
- **Complete** – Total compromise of system integrity; there is a complete loss of system protection, resulting in the entire system being compromised
## CVSS Availability Impact

Measures the impact to availability of a successfully exploited vulnerability. Availability refers to the accessibility of information resources. Attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of a system.

- **None** – There is no impact to the availability of the system
- **Partial** – There is reduced performance or interruptions in resource availability (example: a network-based flood attack that permits a limited number of successful connections to an Internet service)
- **Complete** – Total shutdown of the affected resource; the attacker can render the resource completely unavailable

## CVSS Exploitability

Measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability.

- **Not Defined** – Assigning this value to the metric does not affect the score
- **Unproven that exploit exists** – No exploit code is available, or an exploit is entirely theoretical
- **Proof of concept code** – Proof-of-concept exploit code or an attack demonstration that is not practical for most systems is available
- **Functional exploit exists** – Functional exploit code is available; the code works in most situations where the vulnerability exists
- **High** – Either the vulnerability is exploitable by functional mobile autonomous code, or no exploit is required (manual trigger) and details are widely available; the code works in every situation, or is actively being delivered via a mobile autonomous agent (examples: worm, virus)

## CVSS Remediation Level

Most vulnerabilities are unpatched when first published. Workarounds or hotfixes offer interim remediation until a patch or upgrade is made available. These remediation stages adjust the temporal score downwards, reflecting the decreasing urgency as remediation becomes final.

- **Not Defined** – Assigning this value to the metric does not affect the score
- **Official Fix** – Complete vendor solution is available, through an official patch or upgrade
- **Temporary Fix** – An official, but temporary, fix (examples: hotfix, workaround)
- **Workaround** – Unofficial, non-vendor solution (examples: user-created patch or workaround)
- **Unavailable** – No solution available
CVSS Report Confidence

- **Not Defined** – Assigning this value to the metric does not affect the score
- **Unconfirmed** – Unconfirmed source or conflicting reports; little confidence in the validity of the reports
- **Uncorroborated** – Non-official sources, which can include independent security companies or research organizations
- **Confirmed** – Acknowledged by the vendor or author of the affected technology; it might also be confirmed by widespread exploitation

---

### How XCCDF/OVAL benchmark scans work

McAfee Vulnerability Manager supports XCCDF/OVAL Benchmark scans and can output an XCCDF-compatible XML file and an HTML report. The XCCDF-compatible XML file can be imported into other XCCDF-compatible products.

### OVAL overview

The Open Vulnerability and Assessment Language (OVAL) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified system state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

The OVAL community has developed three schemas written in Extensible Markup Language (XML) to serve as the framework and vocabulary of the OVAL Language. These schemas correspond to the three steps of the assessment process:

- An OVAL System Characteristics schema for representing system information.
- An OVAL Definition schema for expressing a specific system state.
- An OVAL Results schema for reporting the results of an assessment.

Content written in the OVAL Language is located in one of the many repositories found within the community. One such repository, known as the OVAL Repository, is hosted by The MITRE Corporation. It is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions. Each definition in the OVAL Repository determines whether a specified software vulnerability, configuration issue, program, or patch is present on a system.

The information security community contributes to the development of OVAL by participating in the creation of the OVAL Language on the OVAL Developers Forum and by writing definitions for the OVAL Repository through the OVAL Community Forum. An OVAL Board consisting of representatives from a broad spectrum of industry, academia, and government organizations from around the world oversees and approves the OVAL Language and monitors the posting of the definitions hosted on the OVAL website. This means that OVAL, which is funded by US-CERT at the US Department of Homeland Security for the benefit of the community, reflects the insights and combined expertise of the broadest possible collection of security and system administration professionals worldwide.
The OVAL language is a collection of XML schema for representing system information, expressing specific system states, and reporting the results of an assessment. The OVAL Repository is the central meeting place for the OVAL Community to discuss, analyze, store, and disseminate OVAL Definitions.

An OVAL Definition file consists of sections that contain Definitions, Tests, Objects, States, and Variables. This layout organizes:

- Individual components needed to describe a check on a target (Definitions).
- How to evaluate that check (Tests).
- What data to collect from that check (Objects).
- The desired result of that check (States).
- How to store intermediate results and even pass parameters into the file (Variables).

All OVAL checks have a unique identifier. This identifier must be unique across the entire OVAL document, and should be unique across the OVAL community.

Note: For more information about the McAfee Vulnerability Manager XCCDF/OVAL implementation and usage, refer to the McAfee Vulnerability Manager documentation on the ServicePortal at http://mysupport.mcafee.com.

OVAL links

CCE
CCE is a format to describe system configuration issues in order to facilitate correlation of configuration data across multiple information sources and tools.

- CCE specification: http://cce.mitre.org
- CCE schema location: http://cce.mitre.org

CPE
CPE is a structured naming scheme for IT platforms (hardware, operating systems, and applications) for the purpose of identifying specific platform types.

- CPE specification: http://cpe.mitre.org
- CPE schema location: http://cpe.mitre.org/specification/index.html
- CPE dictionary: http://nvd.nist.gov/cpe.cfm

CVE
CVE is a format to describe publicly known information security vulnerabilities and exposures. Using this format, new CVE IDs are created, assigned, and referenced in content on an as-needed basis without a version change.

- CVE website: http://cve.mitre.org
- CVE dictionary: http://nvd.nist.gov/

CVSS
CVSS is a scoring system that provides an open framework for determining the impact of information technology vulnerabilities and a format for communicating vulnerability characteristics.

- SCAP CVSS base scores: http://nvd.nist.gov
OVAL
OVAL is an XML-based language used for communicating the details of vulnerabilities, patches, security configuration settings, and other system states in a system-readable form.

XCCDF
XCCDF is an XML-based language for representing security checklists, benchmarks, and related documents in a system-readable form. An XCCDF document represents a structured collection of security configuration rules for one or more applications and/or systems.

- XCCDF specification: http://nvd.nist.gov/xccdf.cfm
- XCCDF schema location: http://nvd.nist.gov/xccdf.cfm

Working with XCCDF and OVAL
Here is an overview of the XCCDF process in McAfee Vulnerability Manager.

1. Update your XCCDF content, if necessary.
2. Set up an XCCDF Benchmark scan.
3. Run the XCCDF Benchmark scan.
4. View the results.

Here are some things to remember when using the product XCCDF tool.

- You cannot edit benchmarks, profiles, or OVAL checks in the product.
- XCCDF reports allow one benchmark and profile at a time.
- McAfee provides some McAfee standard SCAP content. McAfee standard SCAP content cannot be deleted from the product.
- McAfee Vulnerability Manager has no direct support for CVSS customization. Use the CVSS Calculator link to calculate custom CVSS scores. CVSS scores are part of the vulnerability details report.

XCCDF tab
The eXtensible Configuration Checklist Description Format (XCCDF) provides a format for specifying security checklists, benchmarks, and related configuration guidance as a way of promoting good security practices. An XCCDF XML document is a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing.

McAfee Vulnerability Manager does not provide a way to modify an XCCDF XML file.

Features and settings
The XCCDF tab allows you to import, update, delete, and view XCCDF XML files.

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import File</td>
<td>Import an XCCDF XML file</td>
</tr>
</tbody>
</table>
Working with McAfee Vulnerability Manager Scans
How XCCDF/OVAL benchmark scans work

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
</table>
| Action         | ![View XML](View XML)
|                | Displays the contents of the selected XCCDF XML file in a new window. For the McAfee SCAP content generated date, look for the Status Date in the XML file. |
|                | ![Update](Update) – Allows you to import an updated XML file for the selected benchmark. |
|                | ![Delete](Delete) – Remove a benchmark from the XCCDF tab. |

**Note**: Once a benchmark has been uploaded, you can only update the benchmark. The benchmark unique ID is based on the file name and the benchmark ID in the XML file. To upload a benchmark with new content, you must delete the existing benchmark first.

<table>
<thead>
<tr>
<th>Benchmark ID</th>
<th>The benchmark ID for the benchmark.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>The file name for the XML file uploaded into the product.</td>
</tr>
<tr>
<td>Upload Time</td>
<td>The date/time stamp of the latest upload for this check.</td>
</tr>
<tr>
<td>View per page</td>
<td>Select the number of XCCDF items to view on the page.</td>
</tr>
</tbody>
</table>

**Import an XCCDF file**

**Note**: Once a benchmark has been uploaded, you can only update the benchmark. The benchmark unique ID is based on the file name and the benchmark ID in the XML file. Changing the XCCDF file name does not allow you to import the same XCCDF benchmark ID under a different name; attempting this only updates the existing XCCDF data. To upload a benchmark with new content, you must delete the existing benchmark first.

1. Log on as the Global Administrator.
2. Select **Manage | XCCDF/OVAL**.
3. Click **Import**.
4. Click **Browse** to navigate to and select the appropriate file.
5. Click **Open**. The path and file name appear in the field.
6. Click **Upload File**. In the Quick View area, you can see which file is going to be imported. A brief description should also be available.
7. If necessary, select file commit options.
   **Validate?** – Before committing a file to McAfee Vulnerability Manager, the file is validated against a schema or schematron. If the file fails schema validation, an error message appears and the file is not committed to the product. If necessary, view the log file for more information about the validation failure.
8. Click **Commit File**. The contents of the file are added to the product. A File Successfully Committed message appears.
9. Click **Exit XCCDF Upload**.
OVAL tab

The Open Vulnerability and Assessment Language (OVAL) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

OVAL information appears in the McAfee Vulnerability Manager XCCDF Benchmark scan report.

McAfee Vulnerability Manager does not provide a way to modify an OVAL XML file.

Features and settings

The OVAL tab allows you to import, update, delete, and view OVAL XML files.

<table>
<thead>
<tr>
<th>Column heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import File</td>
<td>Import an OVAL XML file</td>
</tr>
<tr>
<td>Action</td>
<td>• View XML – Displays the contents of the selected XML file in a new window. For the OVAL content generated date, look for the oval:timestamp tag in the XML file. • Update – Allows you to import an updated XML file. • Delete – Remove a file from the OVAL tab.</td>
</tr>
<tr>
<td>Name</td>
<td>The file name for the XML file uploaded into the product.</td>
</tr>
<tr>
<td>Upload Date</td>
<td>The date/time stamp of the latest upload for this check.</td>
</tr>
<tr>
<td>View per page</td>
<td>Select the number of OVAL items to view on the page.</td>
</tr>
</tbody>
</table>

Import an OVAL file

Use the following task when importing an OVAL file.

1. Log on as the Global Administrator.
2. Select Manage | XCCDF/OVAL.
3. On the OVAL tab, click Import.
4. Click Browse to navigate to and select the appropriate file.
5. Click Open. The path and file name appear in the field.
6. Click Upload File. In the Quick View area, you can see which file is going to be imported. A brief description should also be available.
7. If necessary, select file commit options.
   Validate? – Before committing a file to McAfee Vulnerability Manager, the file is validated against a schema or schematron. If the file fails schema validation, an error message appears and the file is not committed to the product. If necessary, view the log file for more information about the validation failure.
8. Click Commit File. The contents of the file are added to the product. A File Successfully Committed message appears.
9. Click Exit OVAL Upload.
CPE tab

The Common Platform Enumeration (CPE) is a structured naming scheme for information technology systems, platforms, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a language for describing complex platforms, a method for checking names against a system, and a description format for binding text and tests to a name.

McAfee Vulnerability Manager allows you to upload, view, and commit a CPE XML file. The CPE file can only be uploaded, there are no options to edit or delete this file. The CPE can be updated using FSUpdate or by using the import tool to manually update the CPE file.

The product uses the standard CPE dictionary and four custom CPE entries. The four custom CPE entries are: printer, router, unknown, and unix. These are items that the product can return information on that are not part of the standard CPE dictionary.

McAfee Vulnerability Manager Custom CPE entries

<table>
<thead>
<tr>
<th>CPE entry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpe:/o:mcafee_vulnerability_manager:unknown</td>
<td>The product was unable to uniquely identify the operating system.</td>
</tr>
<tr>
<td>cpe:/o:mcafee_vulnerability_manager:printer</td>
<td>Generic network-attached printer device.</td>
</tr>
<tr>
<td>cpe:/o:mcafee_vulnerability_manager:router</td>
<td>Generic network-attached router device, CISCO or other vendor.</td>
</tr>
</tbody>
</table>

Importing a CPE file

Use the following task to import a CPE file.

1. Log on as the Global Administrator.
2. Select Manage | XCCDF/OVAL.
3. Click the CPE tab.
4. Click Browse to navigate to and select the appropriate file.
5. Click Open. The path and file name appear in the field.
6. Click Upload File. In the Quick View area, you can see which file is going to be imported. A brief description should also be available.
7. Click Commit File. The contents of the file are added to McAfee Vulnerability Manager. A File Successfully Committed message appears.
8. Click Exit CPE Import.

SCAP tab

The Security Content Automation Protocol (SCAP) is a method for using specific, open standards to enable automated vulnerability management, measurement, and policy compliance evaluation. SCAP provides a means of measuring systems to find vulnerabilities and offer methods to score those findings in order to evaluate the possible impact.
McAfee Vulnerability Manager allows you to upload and commit an SCAP file. The SCAP file must be in a ZIP format. The SCAP file can only be uploaded, there are no options to edit or delete this file. The SCAP file can be updated using the import tool to manually update the file.

**Importing a SCAP file**

Use the following task when importing an SCAP file.

1. Log on as the Global Administrator.
2. Select Manage | XCCDF/OVAL.
3. Click the SCAP tab.
4. Click Browse to navigate to and select the appropriate file.
5. Click Open. The path and file name appear in the field.
6. Click Upload File. In the Quick View area, you can see which files are going to be imported. A brief description should also be available.
7. If necessary, select file commit options.
   - Force Update – Overwrite the existing with the file being committed.
   - Validate? – Before committing a file to McAfee Vulnerability Manager, the file is validated against a schema or schematron. If the file fails schema validation, an error message appears and the file is not committed to the product. If necessary, view the log file for more information about the validation failure.
8. Click Commit All Identified Files. The contents of the file are added to the product. A File Successfully Committed message appears.
9. Click Exit SCAP Import.

**Using the United States Federal Information Processing Standard**

The United States Federal Information Processing Standard (FIPS) is a security requirement for computers used by the United States federal government. The FIPS 140-2 standard defines cryptographic algorithms and requirements for generating keys. McAfee Vulnerability Manager supports the use of the FIPS 140-2 standard.

When the server operating system is configured for FIPS 140 compliant mode, users cannot access the enterprise manager if TLS 1.0 is not enabled in their web browser. To enable TLS 1.0 on the client system, use the following procedure.

**Enable TLS 1.0 on the client system**

For further information, see the Microsoft KB article about FIPS security settings in Windows XP and later versions at [http://support.microsoft.com/kb/811833](http://support.microsoft.com/kb/811833).

1. In Internet Explorer, select Tools | Internet Options.
2. Select the Advanced tab and navigate to Security.
3. Make sure the following checkboxes are selected:
   - Use SSL 2.0
   - Use SSL 3.0
   - Use TLS 1.0
4. Select Apply, then select OK.
FDCC compliance scans

FDCC Compliance Scans search for vulnerabilities that would impact compliance with the Federal Desktop Core Configuration (FDCC).

To configure your Windows Policy Manager with FDCC compliance settings, do the following:

- Export the Windows Policy settings, to save it for future use.
- Import the FDCC XML file.
- Run a scan using the FDCC scan template.

Export Windows Policy settings

Export your current Microsoft Windows Policy settings (to save these settings for future use).

1. Log on to the enterprise manager as the Global Administrator, then select Manage | Policy.
2. Click Config, then click Export to XML. A File Download message displays.
3. Click Save, then navigate to a folder to save your policy settings as a compressed file. If you want to import these settings, you must decompress the file.
4. Click Save.

Import FDCC XML file

Import the FDCC settings from a McAfee XML file.

1. Download the FDCC XML file from the download site (https://secure.nai.com/apps/downloads/my_products/login.asp) (requires a grant number).
2. Log on to the enterprise manager as the Global Administrator.
3. Select Manage | Policy.
4. Click Config.
5. Click Browse, select the FDCC XML file, then click Open.
6. Click Import from XML.
7. Click OK.

Run FDCC scan template

After configuring your Windows Policy Manager, run an FDCC Audit Scan.
1. Log on to the enterprise manager as a user who can create scans. The Global Administrator cannot create a scan.

2. Select Scan | New Scan.

3. Select Use a McAfee Template, then select Federal Desktop Core Configuration Windows Vista Audit Scan or Federal Desktop Core Configuration Windows XP Audit Scan.

4. Click Next.

5. Type a name for the scan and add targets to the scan.

6. Click Next.

7. Modify your settings, then click Next.

8. Select your report options, then click Next.

9. Set a schedule for the scan, then click Schedule Scan. If you don’t activate your scan, click Save. If you set your scan to run immediately, click Save and Scan Now.

**SUDO scans**

Administrators can run commands in privileged mode with SUDO instead of SU.

SUDO means substitute user do and is a program for UNIX operating systems. It allows users to run programs with the security privileges of another user.

**Configure SUDO**

Using SUDO and the product requires some configuration.

The procedure for configuring SUDO settings vary based on the operating system, so only the settings are listed instead of providing procedure steps.

The configuration requirements are:

- lecture=never
  Lecture is a message that appears when using root access that lets the user know to be careful when using root access.

- listpw=never
  List password requires a password to be typed whenever the list of commands is requested.

- verifypw=always

- The default failed password text must not be changed.

- The account used to authenticate has a shell that does not contain any markup. For example, no text color.

When using SUDO with the product, there are other configuration conditions that might affect your scans.

- If you are using SUDO 1.6, you configured targetpw in your SUDO configuration, and you are trying to elevate the user to something other than root, your access is denied on your SUDO scans.

- If you are using SUDO 1.7, you have not configured targetpw, or you're using root as your elevated user, your access works on your SUDO scans.

- The product does not support elevating to multiple users. You can only elevate to the credentials you provide in the SUDO Privileged Access fields.

- If SUDO is selected, all commands are executed using SUDO, even if root credentials are provided under Account Type.
Use SUDO in credential sets and scan configurations

When creating a shell credential in a credential set or a scan configuration, including a SUDO user name or password overrides the user name or password under Account Type.

A SUDO user name and password only provide the privileges of another user, not log in access to a system. You must provide a user name under Account Type and that user name must be configured for SUDO.

This task describes only the new SUDO feature related to credentials in a scan configuration and credential sets. For information and tasks about the credential process, see the product documentation or online help.

1. Create or edit a credential or credential set.
2. Select Shell Domain, Shell Individual, or Shell Default.
3. Type a user name under Account Type.
5. The rest of the shell credential configuration depending on how SUDO is configured.
   - **Account Type password** – Used to log in to the asset. If left blank, then a certificate is used. Certificates must be properly configured.
   - **Privileged Access user name** – The user name used for SUDO. If left blank, then the Account Type user name is used.
   - **Privileged Access password** – The password used for SUDO. If left blank, then the Account Type password is used.

   **Note:** When using a certificate for authentication, you must provide the SUDO credentials under Privileged Access.

6. Click Save.

Oracle on non-standard ports

The product can detect the Oracle Transparent Network Substrate (TNS) protocol running on non-standard ports.

Add Oracle on a non-standard port to a scan configuration

These steps describe how to add assessing the Oracle Transparent Network Substrate (TNS) protocol running on non-standard ports in a scan configuration. For steps on how to create a scan configuration, see the product guide.

1. Create a new scan or edit an existing scan.
2. On the Settings tab, click Services, then click Advanced Options.
3. Make sure Detecting services running on non-standard ports is selected.
4. Select tns under Available Services, then click >> to add it to Selected Services.
5. Click Close.
6. Under TCP Scanning, select Custom.
7. Type the custom port number, separating the numbers with a space.
8. Save your scan.
How web application scans work

McAfee Vulnerability Manager provides a scan configuration, vulnerability checks, and scan reports for web applications.

The web application scan searches for vulnerabilities that include buffer overflows, cross site scripting, and unauthorized access. When the web application scan creates an asset, the asset is associated with the URL and not with the IP address of the web server.

Because a web server can host multiple web applications, associating the web asset with the URL provides a unique identifier. A web asset is created when you create a web asset manually, add a URL to a web application scan configuration, or run a discovery scan that discovers the web server.

Providing credentials to a web application scan allows authorized access to the site. Links on the logon page are also tested for vulnerabilities.

If you do not provide credentials to a web application scan, the scan runs checks for unauthorized access to the site. Links on the logon page are also tested for vulnerabilities.

Note: Web asset information includes the IP address for the web server, on things like the asset page and in reports. Deleting the web server also removes the IP address from the web asset information. Also, it is possible to create asset filters using the web server IP address to search for web assets running on that server, but deleting the web server asset breaks that asset filter.

Create web application configurations

Web application configurations (WebAppConfigs) allow you to specify the URLs to include or exclude, the parameters to exclude, and specify which HTTP and HTTPS ports to use.

Web application configurations can be selected when creating a scan configuration. This can save you time if you use the same web application configuration in different scan configurations.

Creating web application configurations also saves you time if you need to change or update your web application settings. Instead of changing the web application settings in the different scan configurations, you can change the web application configuration.

1. Log on as the Root Organization Administrator, then select Components | Web App Configs.
2. Click Create New.
3. Type a unique name for this web application configuration and an optional description.
4. To allow Workgroup Administrator to use this web application configuration, select Public.
5. Click Next. The Settings tab appears.
6. In the Entry Paths field, type any paths you want to use as a starting point for a scan. Entry paths are case-sensitive.

Adding entry paths ensures the web application scan covers all the paths you want, especially if the entry path is not linked to the web application you typed in a scan configuration. The entry path is added to the web application target you typed in a scan configuration. The scan doesn't scan any folders above the path specified.

For example: If you entered http://webappname.com/consumer/product/ as your target in a scan configuration and you add /admin/ to the Entry Path field, the scan doesn't scan the path http://webappname.com/admin/, because this is above the path specified as the target.
7 Type one path per line. Press Enter to add a line.
8 In the Exclude Paths field, type the path of any web folder or web page within the web application that you do not want to scan. Exclude paths are case-sensitive. Entries in the Exclude Path field are added to the URL included with a web application scan. Do not type a full URL as an excluded path.

For example: If you want to exclude the Admin folder from your scan (http://webappname.com/admin/), typing the following examples produces the described results.
- /admin – This excludes anything that has "/admin" in it, including any files or pages. (http://webappname.com/registration/administrationform.php is excluded, even if you wanted it as part of your scan results).
- /admin/ – This excludes any folders labeled "/admin/".

9 Type one path per line. Press Enter to add a line.
10 In the Exclude parameters field, type any web parameters within the web application that you do not want to scan. Type one parameter per line. Press Enter to add a line.
For example: If you use a session ID, you should exclude that parameter from the scan configuration. Otherwise, McAfee Vulnerability Manager changes the session ID, to check for vulnerabilities, and web application could terminate the session before the scan is complete.

11 Use the Ports Pairs fields if you have specific HTTP and HTTPS ports for the web application. You can only type one HTTP port and one HTTPS port per web application configuration.
12 Click Save.

Create a web application scan

Creating a web application scan is similar to other McAfee Vulnerability Manager scan configurations. The Web App Config settings are different on the Settings tab of a scan configuration.

Tip: If you want to use the asset settings in a scan configuration (like the port number), scan the asset instead of a URL that matches the asset.

1 Select Scans | New scan.
2 On the Scan details page, select Use a McAfee Vulnerability Manager template.
3 Select a web scan template, then click Next.
   - CWE/SANS Top 25 Scan – Searches for the CWE/SANS Top 25 most dangerous programming errors/vulnerabilities in web applications.
   - Deep Web Scan – Performs the most thorough web application assessment possible without constraints such as time limitations.
   - Informational Web Crawl – Indexes your web application and provide informational level vulnerabilities.
   - Light Web Scan – Performs a quick web application assessment of the most critical vulnerabilities within a two hour time period.
   - OWASP Top 10 Scan – Searches for a broad consensus of what are considered the most critical web application security flaws listed in the OWASP Top 10 list.
   - PCI DSS Compliance Scan – Searches for vulnerabilities that would impact compliance with the Payment Card Industry (PCI) Data Security Standard.
4 On the Targets tab, type a unique scan name. Typing a description is optional.
5 Type the URL of the web application you want to scan, then click Next. You can also browse or search for a web application asset.
   - Type the full URL (example: http://www.hostname.com), otherwise the product scans this system as an asset and not a web application.
   - You should scan one web application per scan configuration because one web application could lead to multiple web pages, with scan data returned for each page.
   - A URL is validated when the scan runs, not when the scan is created. During a scan, if a URL resolves to an IP address that is outside your IP range, it is not scanned.
When adding the same web application to two different scans, if the URLs differ, the product might consider each URL as an asset that requires a license.

For example: If http://myhost.com and http://myhost.com/cmdinjection/ are added to different scans, this web application would be treated as two different assets, each requiring a license.

A URL can be case-sensitive, so the product creates individual web application assets for the same URL with different cases.

For example: http://myhost.com/CMDinjection/ and http://myhost.com/cmdinjection/ are treated as two different assets, each requiring a license.

6 Click the icon on the left side of the page to change the settings, then click Next.

Hosts – Specify options for ICMP, UDP, and TCP scanning Also select/deselect the Asset Tagging option.

The product expects ICMP, UDP, or TCP. If these are not being used, you must specify a non-standard port or the asset is not assessed.

Services – Specify the services you want discovered on your network

Credentials – Create and manage credentials used to access systems on your network

Vuln Selection – Specify the vulnerabilities you want checked under the General, Windows, Wireless, and Shell categories

Some web vulnerability checks appear under multiple web vulnerability categories. Selecting a web vulnerability check under one category selects that same web vulnerability check in other categories.

For example: Web Server uses Basic Authentication is under Authentication and Information Crawl-Only Vulnerabilities. Selecting either web vulnerability category selects this specific web vulnerability in the other category.

Optimize – Change settings to optimize the performance of the product

Web App Config – Specify the entry paths, exclude paths, exclude parameters, and port pairs for web application scans

Override asset settings (use scan’s settings against all targets) – If any of the web applications in the scan configuration have an existing web application configuration, selecting this option overrides that configuration and use the web application settings on this page.

Use asset settings (use scan’s settings as defaults for targets without their own settings) – Any web application in the scan configuration without an existing web application configuration uses the settings on this page. All web applications with an existing web application configuration uses the existing configuration.

Use Existing Config – All existing web application configurations appear in a drop-down list.

Entry Paths – The web address to use as a starting point for the scan configuration. Type one URL per line. Press Enter to add a line.

Exclude Paths – Any web addresses within the web application that you do not want to scan are typed in here. Type one URL per line. Press Enter to add a line.

Exclude Parameters – Any web parameters within the web application that you do not want to scan are typed in here. Type one parameter per line. Press Enter to add a line.

For example: If you use a session ID, you should exclude that parameter from the scan configuration. Otherwise, the product changes the session ID, to check for vulnerabilities, and web application could terminate the session before the scan is complete.

Port Pairs – If you have specific HTTP and HTTPS ports for the web application, type those ports here. Only one HTTP port and one HTTPS port per scan configuration.
Specify if you want to create remediation tickets for this scan when it has completed running. Deselect the checkbox if you do not want remediation tickets created.

Select theFoundScore Type you want used for this scan (Internal or External). This setting defines the set of calculations used to determine the FoundScore value.

Select the format in which you want reports created.

Select the report sections you want to include in your report, then clickNext.

Select Active to enable the scan. If you decide to activate this scan and set the Schedule Type to immediate, the scan starts right after you save it. Inactive scans are saved but are not run automatically (you can run them manually by clickingActivate on the scan configuration page).

Select the scan engine.

Note: If the Select Engine displays AutoSelect, the Global Administrator or Root Organization Administrator has enabled automatic scan engine selection.

Select a time zone to coordinate the scan start time.

- Use Engine Time – Uses the time zone the scan engine is in as the start time for the scan configuration.
- Use Local Time – Uses the time zone you select and calculates the start time (based on UTC time).

Note: UTC time is constant. If the selected timezone alters the time (like daylight savings time), the start time for a recurring scan changes.

Schedule the scan to run immediately, at a specific date and time, or on a recurring schedule. To use a Scan Window so that the scan runs during specific hours or on specific days, select the checkbox and type the window details.

Save the scan.

- Save and Scan Now – Active and Immediate are selected. This saves the scan configuration and starts the scan.
- Schedule Scan – Active and One Time or a recurring schedule are selected. This saves the scan configuration and the scan starts at the scheduled date and time.
- Save – Inactive is selected. This saves the scan configuration without starting the scan.

Add a web asset

Web assets can be added manually to McAfee Vulnerability Manager.

1 Select Manage | Assets.
2 Right-click the group you want to add the web asset to and select Add Asset.
3 Select Enter URL.
4 Type the URL of the web asset. The web path must include HTTP:// or HTTPS:// for the scan configuration to recognize this target as a web application.
   Do not type an IP address. After a scan has discovered the web application asset, the IP address of the server hosting the web application appears on the assets page.
   Web application URLs can be case-sensitive. Adding a URL using a different case counts it as a separate web asset.
5 Type a unique label for the web asset. Selecting a criticality level and owner are optional.
6 Select or type the web application configuration details.
   - Select Web App Config from the drop-down list if you created a web application configuration.
   - Select Use These Settings to type in the details.
   Entry Paths – The web path to use as a starting point for the scan configuration. Adding entry paths ensures the web application scan covers all the paths you want, especially if the entry path is not linked to the web application you entered on the Targets tab.
Exclude Paths – Any web folder or page within the web application that you do not want to scan are typed in here.

Exclude Parameters – Any web parameters within the web application that you do not want to scan are typed in here.

Port Pairs – If you have specific HTTP and HTTPS ports for the web application, type those ports here. Only one HTTP port and one HTTPS port per scan configuration.

Click Submit to save the web asset.
Managing remediation and risk

You can configure McAfee Vulnerability Manager to watch your network as closely as you like. Notifications let you and your staff know when there are problems, and tickets tell you how to fix the issue and track the results. You can also set the system to watch for specific threats on specific networks to heighten security when needed.

Managing notifications

The McAfee Vulnerability Manager Notification Service adds SNMP and email integration for remediation and scan-related events. Remediation tickets are used to manage and track vulnerabilities in systems within your corporate network. The remediation system is available through the enterprise manager and is integrated with other functions of the system, for example, access management.

Note: If you have McAfee VirusScan Enterprise On-Access Scanner enabled, the McAfee Vulnerability Manager Notification Service fails to connect to your email server. To receive email notifications, exclude the notification service from VirusScan Enterprise. See the McAfee Vulnerability Manager Installation Guide for further information about using McAfee Vulnerability Manager and McAfee VirusScan Enterprise.

How notifications work

The notification service can be configured to communicate and interact with an external SNMP management node, so you can receive notifications, via SNMP trap, of when specific events occur. Event notifications are sent from the McAfee Vulnerability Manager to your SNMP management console.

The Global Administrator enables or disables notifications, and specifies where and how events are to be sent. Once the Global Administrator has enabled notifications, the Root Organization Administrator specifies the events for which notifications are to be sent.

Enable notifications (Global Administrator only)
The Global Administrator must enable and configure the SNMP and email notification settings.

1. Log on and select Manage | Notifications.
2. Specify if event notifications are to be sent when tickets are generated or when they are assigned for export.
3. Enable or disable SNMP notifications.
4. Specify the SNMP manager and agent.
5. Enable or disable email notifications.
6. Specify the email server settings and email addresses.
7. Click Save. To cancel any changes made, click Reset.
Enable notification per organization
After the Global Administrator enables notifications, the Root Organization Administrator must specify which ticketing events are sent as SNMP or email notifications.

1. Log on and select **Manager | Notifications**.
2. Select the **Org Settings** tab.
3. Specify the type of notification (SNMP or email) for ticketing and scan related events.
4. Click **Save**. To cancel any changes made, click **Reset**.

Enable notifications per user
After the Global Administrator enables notifications, the Root Organization Administrator, Workgroup Administrator, Remediation Administrator, and Default (remediation-only) User must specify which ticketing events send a notification.

1. Log on and select **Manage | Notifications**.
2. Specify the ticketing events for which you want to receive email notifications.
3. Click **Save**. To cancel any changes made, click **Reset**.

**Specifying organization settings**

When creating notifications, you can specify the remediation and scan-related events to be sent as email notifications to the organization.

![Notification Settings – Organization Settings](image)

**Set Remediation Related Events**

1. Log on as the Root Organization Administrator.
2. Select **Manage | Notifications**, then select the **Org Settings** tab.
3. Select the checkbox for the type of notification (SNMP or email) to use for each ticketing related event.
4. Click **Save**. To cancel any changes made, click **Reset**.

**Set Scan Related Events**

1. Log on as the Root Organization Administrator.
2. Select **Manage | Notifications**, then select the **Org Settings** tab.
3. Select the checkbox for the type of notification (SNMP or email) to use for each scan related event.
4. Click **Save**. To cancel any changes made, click **Reset**.
Specifying user settings

When creating notifications, you can specify the remediation and scan-related events to be sent as email notifications to selected users.

![Figure 14: Notification Settings – User Settings](image)

Select remediation and scan related events for notifications

1. Select **Manage | Notifications**.
2. Select the checkbox for each event for which you want to receive notifications. To disable notifications, deselect the checkbox.

   **Note:** The scan related events you select apply to each scan selected. For example, if you select to receive notifications for **Scan Started**, you receive a notification each time every scan you selected is started.

3. Select the scans you want to receive notifications for each event selected.
4. Click **Save**. To cancel any changes made, click **Reset**.

Specify when to send event notifications

For event email notifications, select the events you want to receive notifications for.

1. Log on as the Global Administrator and select **Manage | Notifications**. The Notification Settings page appears.
2. Select when to send a notification.
   - **Ticket Generated**
   - **Ticket Assigned for Export**
3. Click **Save**.

![Figure 15: Notification Settings – General Settings](image)
Enabling SNMP notifications

Before you can send email notifications, you must specify SNMP manager and agent settings. Enabling SNMP settings must be done by the Global Administrator.

Select the **Enable SNMP Notifications** checkbox to enable SNMP notifications. Then complete the remaining information, specifying the SNMP version, and incoming and outgoing SNMP settings.

Log on as the Global Administrator, then select **Manage | Notifications**. The Notification Settings page appears.

SNMP general settings
- **SNMP version** – Click the arrow to specify the SNMP version (1 or 2c).
- **Community string** – Type the SNMP community string.
- **Throttle** – Click the arrow to select the throttle (number of maximum messages per second).

Incoming SNMP settings
- **Address** – Type the listening IP address, fully-qualified domain name, or host name of the SNMP agent that is to receive incoming SNMP messages from an external SNMP manager.
- **Port** – Type the listening port number or IP address.
- **Senders list** – Type the names of authorized senders of SNMP messages. For example, you might want to type the name of the outgoing SNMP management node here, so that the McAfee Vulnerability Manager Notification Service listens to messages sent by that SNMP management node. If you do not type a name in this field, no messages are processed by the McAfee Vulnerability Manager Notification Service.
  - **Add** – Click this button to add the name in the senders list.
  - **Remove** – Select a name in the senders list and click **Remove** to remove the name from the list.
  - **Allow verify vulnerability** – Select this checkbox if you want McAfee Vulnerability Manager to respond to SNMP trap messages requesting verification of a vulnerability.

Outgoing SNMP settings
- **Address** – Type the IP address, fully-qualified domain name, or host name of the SNMP management node the product sends SNMP messages to.
- **Port** – Type the port number of the SNMP management node.
Enable email notifications

Before you can send email notifications, you must specify email server settings. Only the Global Administrator can enable email notifications.

1 Log on as the Global Administrator, then select Manage | Notifications. The Notification Settings page appears.
2 Select Enable Email Notifications to enable email notifications. Then complete the remaining information, specifying the email server address, and the email addresses of the sender/recipient.
3 Click Save.

Note: Email notifications for updates applied via the configuration manager are sent to the address listed for Vulnerability Manager Operations. If you have enabled email notifications in the configuration manager Preferences, be sure to include an email address in the McAfee Vulnerability Manager Operations field.

Email server
- **Address** – Type the address of the mail server. Use the IP address, fully-qualified domain name, or host name of the server (up to a maximum of 256 characters).
- **Throttle** – Sets the maximum number of messages allowed per second.
- **Port** – Type the port number of the mail server to which notification messages are to be sent.
- **Server requires authentication** – Select this checkbox to log on to the mail server with a user name and password.
- **Username** – Type the user name required to log onto the mail server. The user name can be up to 64 characters long.
- **Password** – Type the password associated with this user name. The password can be up to 128 characters long.
Email messages
- **Header message** – The header message is optional.
  Type your organization's security banner here. While McAfee Vulnerability Manager controls the bodies of these messages, you can configure an opening statement as needed. For example, you could include internal contact information or policy notices.
  The maximum number of characters allowed is 256. The email header message can include alphanumeric characters plus underscores, periods, parentheses, hyphens, spaces, commas, slashes (/), and colons.
- **Footer message** – The footer message is optional.
  While the product controls the bodies of these messages, you can configure a closing statement as needed. For example, you could include internal contact information or policy notices.
  The maximum number of characters allowed is 256. The email footer message can include alphanumeric characters plus underscores, periods, parentheses, hyphens, spaces, commas, slashes (/), and colons.

Event and address settings
The following settings apply to each notification type: Ticket Integration, McAfee Vulnerability Manager Operation, User Remediation, and User Scan Status.
- **From name** – Type the name of the sender. This is the person or organization that the email appears to be coming from. Use up to 64 characters.
- **From address** – Type the email address of the person or organization sending the email. If the recipient replies, the reply is sent to this email address. Use up to 256 characters using a proper format (first.last@yourcompany.com).
- **To name** – Type the name of the person or organization who receiving a notification email for this type. Use up to 64 characters.
- **To address** – Type the email address of the recipient that is to receive event notifications. Use up to 256 characters using a proper format (first.last@yourcompany.com).

Notifications for scan and engine related events
McAfee Vulnerability Manager provides SNMP and email notifications for things that happen with ticketing, scans, and the scan engine. This release provides some new email notifications.

**Scan related events (User Settings and Org Settings)**
- **Scan excessive runtime** – Sometimes scans might hang. Most of the time when a scan appears to be hung, it is just taking a long time to finish, leading to an excessive runtime. Selecting the **Scan excessive runtime** notification sends an email when the current scan time is three times longer than the previous time the same scan was run.

- **Scan contains no results** – An email is sent when a scan returns zero vulnerabilities found. This excludes a scan configuration that does not have any vulnerabilities selected, like a Discovery Scan, which is designed to discover only assets on your network.

- **Scan ended in error state** – An email notification is sent when a scan ends in an error state.

**Engine related events (Org Settings)**
- **Engine offline** – An email notification is sent when a scan engine goes offline.

Managing ticketing
As the Root Organization Administrator or Remediation Administrator, you can manage remediation tickets throughout the organization (including workgroups).

The Remediation Management page contains two tabs:
• **Rules** (see "How ticketing rules work" on page 96) – Lets you set up rules to automatically assign remediation tickets to your McAfee Vulnerability Manager users.

• **Global Options** (see "Setting ticketing global options" on page 95) – Lets you determine when remediation tickets should be created, enable the auto-close feature, and set default due dates for tickets--based on their risk level.

The settings on this page affect the entire organization, including all workgroups. Workgroup administrators cannot make changes to these settings.

### How ticketing works

Tickets can be created for vulnerabilities discovered during a scan and these tickets are used to help manage the process of remediating vulnerabilities.

The Root Organization Administrator sets the ticketing options for the organization and can create rules for assigning tickets to users responsible for verifying and fixing any issues.

### Setting ticketing global options

When configuring ticketing rules, you can specify global settings that affect all organizations and workgroups.

The settings on this page affect the entire organization, including all workgroups. Workgroup administrators cannot make changes to these settings.

**Note:** These settings affect the entire organization, including all workgroups. Workgroup administrators cannot make changes to these settings.

### Setting global options

- Select the vulnerability risk level that starts generating tickets.
- Enable or disable the remediation ticket auto-close feature.

![Global Options](image)

**Figure 18: Ticketing – Global Options**

### Global Ticketing settings

- **Create tickets for all vulnerabilities with a risk level higher than or equal to** – Select the level of vulnerabilities that should cause a ticket to be generated.
  - *Informational* – All vulnerabilities produce a ticket.
  - *Low* – Low, medium, and high-risk vulnerabilities produce a ticket.
  - *Medium* – Only medium and high-risk vulnerabilities produce a ticket.
  - *High* – Only high-risk vulnerabilities produce a ticket.

- **Enable automatic closure of tickets whose vulnerabilities have been resolved** – This feature is enabled by default. It automatically closes tickets that are resolved.
Managing remediation and risk
Managing ticketing

**Tip:** Enable this feature to quickly close tickets by verifying them through your regular scanning process.

- **Ticket Default Dates** – Set the default due date for auto-assigned tickets, according to the ticket’s vulnerability risk. For example, setting the high vulnerability risk tickets to 15 days means that if a new high-risk vulnerability is discovered, the ticket resolution is due 15 days after the ticket is created.

**How ticketing rules work**

Create rules that assign tickets to a user automatically, when the tickets are created. In an auto-assignment rule, you determine the action that the rule takes, and you specify the criteria that is used to qualify tickets for that rule. As soon as a ticket is qualified, the rule performs its action on that ticket.

When a ticket is automatically assigned, the details are logged on the ticket details page for that ticket.

This page contains all of the rules that have been created for Ticketing.

The list is empty by default until you add a new rule to it. You can add as many rules as you need. When tickets run through the assignment process, the first rule that matches the ticket determines what action to take for that ticket.

![Remediation Rules List](image)

**Figure 19: Remediation Rules List**

**Rules options**

- **Name** – Shows the name for the rule.
- **Description** – Shows the description for the rule.
- **Status** – Shows if the rule used (Active) or not used (Inactive) for ticket assignments.
- **Edit** – Edits the rule by opening the Rule Editor page.
- **Delete** – Removes the rule from this list and deletes it from the system.

**Note:** If you want to keep the rule, make it inactive instead of deleting it.

- **Run** – Checks through all unassigned tickets for any that match the rule criteria. If any are found, the rule reassigns them according to its settings.
- **Up/Down** – Moves the rule up or down through the list. Ticketing rules run starting at the top of the list. If a ticket is found that matches a rule, it is no longer checked against subsequent rules.

**Use the rule editor**

The Rule Editor lets you specify to whom the tickets are assigned, the tickets' due dates, and the criteria that is used to match tickets to rules.
1. Select Manage | Ticketing, then click Create New Rule.
2. To create a new line of criteria, click Add Criteria.
3. To remove a line of criteria, click Delete on the line you want removed.
4. To automatically assign, export, or ignore a ticket, select the appropriate behavior from the Action drop-down box.
5. To activate the rule, select Active from the Status drop-down box.
6. Click Save.

**Figure 20: Remediation Rule Editor**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Type a name for the rule (up to 50 characters).</td>
</tr>
<tr>
<td>Status</td>
<td><strong>Active</strong> – The rule is used to check all generated tickets.</td>
</tr>
<tr>
<td></td>
<td><strong>Inactive</strong> – The rule remains in the system, but it is not used to make ticket assignments.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description that quickly identifies the rule's actions (up to 256 characters).</td>
</tr>
</tbody>
</table>
Managing remediation and risk
Managing ticketing

Action

**Assign** – Specify the user and due date to which the tickets are assigned.

**Export** – All tickets that meet the criteria are exported. This option is often used with helpdesk systems that create their own tickets from email messages. See the online help for more information on exporting tickets.

**Ignore** – All tickets that meet the criteria are ignored. Scans that discover the same vulnerabilities on the same hosts don’t generate tickets for those vulnerabilities.

Assignee

This option assigns the ticket to the user specified as the action owner* on the Asset Management page in the enterprise manager.

Select the person to whom the tickets are assigned. This list only shows users that have been entered into the system.

Due Date

Determines how long the user has to fix the vulnerability described on the ticket. The number of days is determined from the date that the ticket is discovered.

Add Criteria

Lets you create criteria for the rule. For more information, see To create new criteria (page 99).

*If the rule is set to assign a ticket to an asset owner and the asset owner is not assigned, the rule is ignored so that subsequent rules might be processed. Asset owners are assigned by the Organization Administrator or Workgroup Administrator.

The following table describes the various criteria settings. For each setting, you can select whether to find tickets that match **(Equals)** or that do not match **(Not Equals)**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk</td>
<td>The risk of the vulnerability identified by the ticket can be <strong>high, medium, low, or informational.</strong></td>
</tr>
<tr>
<td>Platform</td>
<td>Type a partial name of the Operating System running on the host. For example, the entry Win matches all versions of the Windows Operating System. The Platform box allows 160 characters, and shows 30.</td>
</tr>
<tr>
<td>Asset Name</td>
<td>If you have assigned asset names to any hosts in the Asset Management module, you can type it here. Typing a partial name applies the rule to any assets that match the partial name. The Asset Name box allows 160 characters, and shows 30.</td>
</tr>
</tbody>
</table>
Asset Criticality  If you have assigned asset criticality ratings to any hosts in the Asset Management module, you can specify the criticality here.

IP Address Range  Type an IP Address range in the format start range – end range. For example, you could type 10.0.0.1-10.0.0.255.

The IP Address Range box allows 160 characters and shows 30.

Vulnerability Name  If you are assigning tickets with specific vulnerabilities, you can type the partial vulnerability name.

Typing a partial name applies the rule to any vulnerabilities that matches the partial name.

The Vulnerability Name box allows 160 characters and shows 30.

Scan Configuration Name  Select the scan from the Scan Name drop-down box.

Make a rule active or inactive

Use the following task to make a rule active or inactive.

1  On the Rules List page, find the rule you want to change and click Edit.
2  In the Rule Editor, select Active or Inactive.
3  Click Save.

Add criteria to a ticketing rule

Set the criteria for the rule by changing the values on each criterion line.

1  Click Add Criteria.
   A new row appears, allowing you to select the options that make up a criterion. You can click Add Criteria again to create as many criteria as you need for the rule.
2  Change the values of the criterion as needed.
3  Click Add Criteria to create another line, or click Save.
4  Click Delete to remove a line.

Figure 21: Ticketing rule criteria list
Managing threats

For managing threats, McAfee Vulnerability Manager provides threat correlation and threat compliance features.

**Threat correlation**
Use threat correlation to quickly respond to threats when and where it matters most in your organization. It enhances your ability to respond rapidly and effectively to critical threats such as coordinated attacks and rampant worms.

The Threat Correlation Module receives Threat Intelligence updates from McAfee Labs, allowing you to immediately correlate these threats with the known open vulnerabilities on your network. This allows you to respond immediately to breaking events. It profiles current threats such as worms, wide-scale attacks, and important new exploits, and correlates these events to your asset and vulnerability information already gathered by the product.

**Threat compliance**
Use threat compliance (on the lower half of the page) to see how compliant your network is for a given threat. The lower half of the page shows how compliant your network is for a given threat. The chart lets you correlate specific threats with specific groups of scans, called Business Units.

*Note:* (N/A) indicates that no hosts were found matching the noted platform, or the selected scan did not include the related FASL checks for the threats.

**Search threats**
Click the Search icon to type a term to search for. The search term must be three characters or longer, and cannot contain * \ , ; . To search for a specific phrase, enclose the search term in quotation marks. The search results are limited to 200 rows.

**How threat correlations work**
A threat is something that can negatively impact a system on your network. Threats range from worms to side-scale attacks.

Correlation reports and the settings you select for Threat Compliance (on this page) are local; they affect what you see through your browser, but do not affect other users. However, the settings on the configuration pages affect all users.

**Use the threat correlations page**
The Threats page allows you to correlate threats with vulnerable hosts, search for threats, and view additional information about threats.

1. Log on as the Root Organization Administrator, then select **Reports | Threats**.
2. Click **Correlate** to correlate the threat with vulnerable hosts.
3. Click **Details** to see more information on how to fix the vulnerability, possible exploits, and additional correlation information.
4. Click the search icon (سلاح), type the text to search for a specific threat, then click **Go**.

*Note:* To search for a specific phrase enclose the search term, including spaces, in quotation marks. For example: "host" might return host, hosts, or hosted; "host " only returns host.

5. Click **Close** to cancel the search.
Use threat correlation

McAfee Vulnerability Manager correlates the results of specific scans to find out which of your systems are susceptible to a threat.

From the **Threats** page, click **Correlate** to open the threat correlation window.

On the threat correlation page:

1. Log on as the Root Organization Administrator and click **Threats**.
2. Click an IP address to view the host details and threats related to the host.

**Note:** The correlation is done by selecting a threat on the Threats page (see "Managing threats" on page 100).

3. Click the download icon in the upper-right corner to download the data (CSV format).

![Figure 22: Threat correlation details](image)

**Correlation features**

- **Risk** – Shows the calculated risk level, given the system and the vulnerability.
- **System** – Shows the name of the vulnerable system.
- **IP Address** – Shows the IP address of the vulnerable system. Click the address to see the host details.
- **Criticality** – Shows the criticality assigned to this host.
- **Matched By** – Shows how the correlation was matched.
- **Operating System** – Shows the operating system running on that host.
- **Vulnerability** – Lists the vulnerability. Click the vulnerability name to see the vulnerability details.

**Set threat configuration user options**

Customize threat correlation to search your network for specific threats using the scans that you specify.

The settings on this page only affect your account. They do not affect others on the system.
1. Log on as the Root Organization Administrator and select **Reports | Threats**.

2. Click **Configure**.

3. Select **Include O/S Mismatches** to include threats that do not match the operating system specified in the threat details. Use this option when the correlation matches the other selected parameters.

   By default, McAfee Vulnerability Manager discards hosts during correlation when the host's operating system does not match the operating system(s) specified in the Correlation Parameters under Threat Details threat definition (details), regardless of a port or service match.

   However, if this option is selected, threats that do not match the operating system specified in the threat details, but match other correlation parameters, are included under Affected Hosts.

4. Select scans under **Threat Correlation Options** to set which scans are reviewing when correlating threats.
Maintaining the database

Microsoft SQL server is a robust and extensible database platform. Although each subsequent release of SQL provides more and more advanced options, the server, database tables, and indices must still be maintained on a regular basis to provide optimal service.

Administrative database maintenance functions

Administrative tasks include starting or stopping the database service, or moving the database files to a new location.

When working with the McAfee Vulnerability Manager Database, the user must have Faultline user access. Faultline is the default name for the database. The Faultline user account is created when the product is installed.

Start and stop the SQL database

Sometimes it is necessary to stop and restart the Microsoft SQL server service, like when you move the database.

Note: If you are unable to connect to the database even after typing the correct server name and credentials, make sure the database is running.

On the database server, you must open the SQL Server Management Studio to check the status of the Microsoft SQL server.

1. Select Start | Programs | Microsoft SQL Server | SQL Server Management Studio.
2. Check the status of the Microsoft SQL server.
   a. If the database icon shows a red square, right-click the icon and click Start.
      When the icon shows a green triangle, the database is running.
   b. If the database icon shows a green triangle, right-click the icon and click Stop.
      When the icon shows a red square, the database has stopped.

Moving the database using SQL Server Management Studio

McAfee recommends using the SQL Server Management Studio to detach and attach a database.

Detach the database

Use the following task to detach a database.
1 Select **Start | All Programs | Microsoft SQL Server | SQL Server Management Studio**.
2 Log on to SQL Server Management Studio.
3 In SQL Server Management Studio Object Explorer, connect to the instance of the SQL Server Database Engine and expand the instance.
4 Expand **Databases**, and select the name of the user database you want to detach.
5 Detaching a database requires exclusive access to the database. If the database is in use, restrict access to a single user:
   a Right-click the database name and point to **Properties**.
   b In the **Select a page pane**, select **Options**.
   c In the **Other options** pane, scroll down to the **State** options.
   d Select the **Restrict Access** option, and in its drop-down list, select **Single**.
   e Click **OK**. If you receive a message that this action closes all connections to the database, click **OK**.
   f Click **OK**.
6 Right-click the database name, then select **Tasks | Detach**. The **Detach Database** dialog box appears.
7 The **Database to detach** grid displays the name of the selected database in the **Database Name** column. Verify that this is the database you want to detach.
8 By default, the detach operation retains any out-of-date optimization statistics when detaching the database; to update the existing optimization statistics, select **Update Statistics**.
9 By default, the detach operation keeps all full-text catalogs that are associated with the database. To remove them, deselect **Keep Full-Text Catalogs**.
10 The **Status** column displays the current database state (**Ready** or **Not Ready**).
   - Before you can detach the database, you must disconnect any active connections by selecting the **Drop Connections** checkbox.
   - If the status is **Not Ready**, the **Message** column displays hyperlinked information about the database. When a database is involved with replication, the **Message** column displays **Database replicated**. When a database has one or more active connections, the **Message** column displays **<number_of_active_connections> Active connection(s)**.
   - To obtain more information about a message, click the hyperlink.
11 When you are ready to detach the database, click **OK**.

**Note**: The newly detached database remains visible in the **Database** node of Object Explorer until the view is refreshed. You can refresh the view at any time: Click in the Object Explorer pane, and from the menu bar select **View**, then **Refresh**.

Attach the database
Use the following task to attach a database.

1 Select **Start | All Programs | Microsoft SQL Server | SQL Server Management Studio**.
2 Log on to SQL Server Management Studio.
3 In SQL Server Management Studio Object Explorer, connect to the instance of the Microsoft SQL Server Database Engine, and expand that instance.
4 Right-click **Databases**, then select **Tasks | Attach**.
5 In the Attach Databases dialog box, to specify the database to be attached, click **Add**; and in the Locate Database Files dialog box, select the disk drive where the database resides and expand the directory tree to find and select the .mdf file of the database; for example: C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\Faultline\faultline.mdf

**Important**: Trying to select a database that is already attached generates an error.
Maintaining the database
Administrative database maintenance functions

6 Optionally, to specify a different name for the database to attach as, type the name in the **Attach as** column of the Attach Databases dialog box.

7 Optionally, change the owner of the database by selecting a different entry in the **Owner** column.

8 When you are ready to attach the database, click **OK**.

**Note:** A newly attached database does not appear in the Databases node of Object Explorer until the view is refreshed. To refresh the view at any time, click in Object Explorer, then click **Refresh** on the View menu.

Moving the database using stored procedures

If you need to move the database using a command line, you can use stored procedures.

**Detach the database**
- Use the **sp_detach_db** system stored procedure to detach the SQL Server McAfee Vulnerability Manager Database.
  - This stored procedure can also run **UPDATE STATISTICS** on all tables before detaching.
- The syntax for **sp_detach_db** system stored procedure is:

  ```sql
  sp_detach_db [ @dbname = ] 'dbname'
  [ , [ @skipchecks = ] 'skipchecks' ]
  ```

**Parameters to the stored procedures**
- [@dbname =] 'dbname' is the database name. 'dbname' is nvarchar(128), a default value is NULL.
- [@skipchecks =] 'skipchecks' The 'skipchecks' parameter determines whether the UPDATE STATISTICS runs or is skipped. The 'skipchecks' is nvarchar(10), a default value is NULL. If 'skipchecks' is true, UPDATE STATISTICS is skipped. If 'skipchecks' is false, UPDATE STATISTICS is run.

**Example**
- The following example detaches the pubs database and runs **UPDATE STATISTICS** on all tables before detaching:

  ```sql
  EXEC sp_detach_db 'pubs', 'false'
  ```

**Attach the database**

When you attach a database, you must specify (at least) the name and physical location of the primary data file. If one or more database files have changed location since the database was detached, you must specify the name and physical location of these files in addition to the primary file.

To attach a SQL Server database, you can use the **sp_attach_db** system stored procedure. The following example shows the syntax for **sp_attach_db** system stored procedure:

```sql
sp_attach_db [ @dbname = ] 'faultline',
[ @filename1 = ] 'filename_n' [ ,...16
]
```

In the above command:
- [@dbname =] 'dbname' is the database name. dbname is nvarchar(128), a default value is NULL.
- [@filename1 =] 'filename_n' is the database file name. filename_n is nvarchar(260), a default value is NULL. There can be up to 16 file names specified.
This is the example to attach the pubs database which contain two files, pubs.mdf and pubs_log.ldf, from the MSSQL\Data directory (e.g. C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data):

```sql
EXEC sp_attach_db @dbname = 'faultline',
    @filename1 = 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\Faultline\faultline.mdf',
    @filename2 = 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\Faultline\faultline_log.ldf'
```

**Attach a single-file database**

A single-file database is a database that only has one data file. In this case, the database can be attached to an instance of SQL Server without using the transaction log file. When the data file is attached, SQL Server creates a new transaction log file automatically.

To attach a single-file database, you can use the `sp_attach_single_file_db` system stored procedure. The syntax for `sp_attach_single_file_db` system stored procedure is as follows:

```sql
sp_attach_single_file_db [ @dbname = ] 'faultline'
    , [ @physname = ] 'physical_name'
```

- `@dbname = 'dbname'` is the database name. 'dbname' is nvarchar(128), a default value is NULL.
- `@physname = 'physical_name'` is the database file name. 'physical_name' is nvarchar(260), a default value is NULL.

This example attaches a single data file of the pubs database from the MSSQL\Data directory (e.g. C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data):

```sql
EXEC sp_attach_single_file_db @dbname = 'pubs',
    @physname = 'C:\MSSQL\Data\pubs.mdf'
```

**Move the database using detach and attach**

Another way to move a database to a different disk or server is to detach the database, copy the database files to the new location, then attach the database referencing the files in the new location.

1. Detach the database using the SQL Server Management Studio, or by using a stored procedure. After detaching, the database is removed from Microsoft SQL Server but is completely intact. You can use these data and transaction log files to attach the database to any instance of Microsoft SQL Server, including the server from which the database was detached.
2. Move the database file(s) to the desired location on another server or disk.
3. Attach the database specifying the new location of the moved file(s). After attaching, the database is available in exactly the same state it was in when it was detached.
Verifying database owner after reattaching

When you reattach a database, the database owner or database users might become detached from the database. If the scan engine cannot connect to the database, use the scan controller in configuration manager to verify that Faultline is the database owner.

Scan Engine cannot connect

When reattaching the database, the database owner can become detached from the database. If the scan engine cannot connect to the database, follow these steps in the enterprise manager to verify that faultline is the database owner.

1. Select Start | All Programs | Microsoft SQL Server | SQL Server Management Studio.
2. Log on to SQL Server Management Studio.
3. Click Logins under the Security folder.

![Figure 23: SQL Server Management Studio – Logins](image)
4 Double-click **faultline**.
5 Select **User Mapping**, then make sure that the Faultline database is selected. Also make sure that the public and db_owner roles are selected.
6 Click **OK** when finished.

![Figure 24: SQL Server Management Studio – Database Access](image)

**Lost users**

When you move the database to another server, and the detached database contains existing users, it is possible to lose users after attaching the database on the new server. To resolve this, manually link the relationship between the user and the appropriate login on the Test server.

You can use the `sp_change_users_login` system stored procedure to link the specified user in the current database to the appropriate login. The following example links the user "Alex" in the current database to the Alex login:

```
EXEC sp_change_users_login 'Update_One', 'Alex', 'Alex'
```

See SQL Server Books Online to get more information about the `sp_change_users_login` stored procedure.
Regular maintenance for database integrity

With every change you make to McAfee Vulnerability Manager, your database changes and grows. There are some things that you can do to help ensure reliable database usage.

Using the following tasks helps ensure reliable database usage from day to day. Some provide automated solutions that the product can help accomplish. Others show things you can do on a daily, weekly, monthly, and as-needed basis. These tasks are intended to catch problems before they occur, and to maintain adequate system performance.

If you should need further assistance or clarification on any of these steps, contact McAfee technical support. The technical support team is available to assist you with this and all other matters relating to the product.

Performing daily tasks

Daily tasks can help track the system status and uncover any immediate problems before they become serious. Because the SQL server application runs on top of the Microsoft Windows operating system, you should pay attention to both environments.

- Monitoring the error logs
- Backing up the database
- Scheduling backups using the Maintenance Plan Wizard
- Monitoring your CPU and memory usage
- Updating statistics

Monitoring error logs

SQL server and Windows produce error logs to help identify problems. Check these logs on a daily basis to spot any inconsistencies that might develop from one day to the next.

Use the Windows Event Viewer

2. Look for any yellow (warnings) or red (stop) errors. These events show you the first indication that something might be wrong with your system.

Any errors should be investigated further. A good place to start is Microsoft’s support site at http://support.microsoft.com.

View the SQL Server logs

SQL Server has its own logs that can be generated and pushed to a text file for review. To produce the logs, open a command line and change directories to the SQL Server location. Once you are there, change directories to the MSSQL \ Binn folder:

- For SQL 2005: C:\Program Files\Microsoft SQL Server\90\Tools\Binn
- For SQL 2008: C:\Program Files\Microsoft SQL Server\100\Tools\Binn

In that directory type the command: SQLDIAG.EXE.

This tool spools its results to a file of the same name and date/time of execution located in the MSSQL\log directory. The output shows where the text file was saved. For example, a SQLDiag report generated on June 23, 2012 has the file name SQLdiag.txt with a modification date of June 23, 2012.

- For SQL 2005: C:\Program Files\Microsoft SQL Server\90\Tools\Binn\SQLDiag
Maintaining the database

Regular maintenance for database integrity

- For SQL 2008: C:\Program Files\Microsoft SQL Server\100\Tools\Binn\SQLDiag

The SQL Server logs provide a wealth of information regarding the SQL server application and the hardware the server is running on. As a side note, it would be a good idea to run this tool and save the output for future reference. The report could be used for testing and documentation of the system.

Backing up the database

Keep backups of your database according to your company policy.


Back up the Transaction Logs using SQL Server Management Studio

Transaction logs are essential to the timely recovery of SQL Server databases. The Full recovery model provides you with better flexibility for recovering databases to an earlier point in time. With Full Recovery model, you should include a transaction log backup in your backup plan.

1 Select Start | All Programs | Microsoft SQL Server | SQL Server Management Studio.
2 Log on to SQL Server Management Studio.
3 Right-click the Faultline database and select Tasks | Back Up from the shortcut menu. The Back Up Database – Faultline window appears.

![Figure 25: Transaction Log Backup](image)

McAfee Vulnerability Manager 7.5 Product Guide 110
4 Type a name for the backup in the **Name** field and an optional description in the **Description** field.

5 To perform a transaction log backup, select **Transaction log** under **Backup type**.

6 Select a destination for the backup. This could be a SQL Server backup device, tape, or a disk file. For example, select a disk file called D:\Backups\Faultline\Faultline_log.bak.

7 To view and, if necessary, modify the transaction log backup options, click the **Options** tab.

8 To remove any previous files with this name and create a new file, select **Overwrite Existing Media**.

9 Select your options, then click **OK**. A progress dialog box appears while the backup is being performed. When the backup is complete, a confirmation dialog box appears.

10 Click **OK**.

**Schedule backups using the Maintenance Plan wizard**

The SQL Server Maintenance Plan wizard utility allows for a backup to be scheduled through the user interface. This wizard is accessed through the SQL Server Management Studio.

For more information on the Maintenance Plan Wizard, see “Database Maintenance Plan Wizard” in SQL Server Books Online.

To use the Maintenance Plan wizard with a McAfee Vulnerability Manager MVM 3100 or MVM 3000 appliance running your database, you must enable Agent XPs and set the SQL Server Agent Service to automatic. See Enable Agent XPs on the database server (page 112).
Enable Agent XPs on the database server

To use the Maintenance Plan wizard with a McAfee Vulnerability Manager MVM 3000 or MVM 3100 appliance running your database, you must enable Agent XPs and set the SQL Server Agent Service to automatic.

Enabling these services is a supported configuration and does not void any warranty on your McAfee Vulnerability Manager appliance.

1. Select **Start | All Programs | Microsoft SQL Server | SQL Server Management Studio**.
2. Log in to SQL Server Management Studio.
3. Click **New Query** and type the following:
   ```sql
   sp_configure 'show advanced options', 1;
   GO
   RECONFIGURE;
   GO
   sp_configure 'Agent XPs', 1;
   GO
   RECONFIGURE
   GO
   ``
4. Click **Execute**.
5. Close SQL Server Management Studio.
6. Select **Start | Administrative Tools | Services**.
7. Right-click **SQL Server Agent**, then select **Properties**.
8. Select **Automatic** for the **Start type**.
9. Click **Apply**, click **Start**, then click **OK**.
10. Close the Services window.

Monitoring CPU and memory usage

Check how the system is using processor and memory resources. If the system is working at 90-100% capacity, additional hardware or systems could improve performance.

Update database statistics

The Configuration Manager contains a database maintenance option that automatically updates the database statistics. Setting this to run daily can help maintain your database performance.

1. From the configuration manager, select **Tools | Preferences**.
2. Click the **Database** tab, then set the **Update Index Statistics**.
   See the online help for more information.

Occasional tasks

Some maintenance tasks can be performed on a weekly, monthly, or as-needed basis.

Weekly monitoring of available disk space

Monitoring available disk space and re-indexing the database can be performed on a weekly basis, to watch for less immediate database issues.
Monitor available disk space
SQL Server has a feature that allows the data and log files to grow as needed automatically. Although this is a benefit, it can have certain drawbacks. Because the application has the ability to adjust the size of the .MDF and .LDF files, the database can run out of room on the hard disk.

1. Select Start | All Programs | Microsoft SQL Server | SQL Server Management Studio.
2. Log on to SQL Server Management Studio.
3. Expand the tree until you see the Faultline Database. To do this, select Databases | Faultline.
4. Right-click the Faultline database and select Properties.
5. In this section, look at the Size and Space Available fields.
   - **Size** indicates how much disk space has been allocated for the database.
   - **Space Available** indicates how much space remains of the amount displayed in the Size field.

   It is very important to monitor these numbers to make sure your database does not run out of room. With the database set to grow automatically, this space can fill up quickly.

Re-index the database
McAfee recommends that you re-index your database once a week. You can do this using Microsoft SQL Server Management Studio.

Run this once each week or when you experience performance degradation. The process is proprietary – you must bring down the database while re-indexing it. The duration depends on the size of the database.

The re-indexing process internally switches the recovery model to simple recovery, then switches back to the original recovery model to prevent the creation of mass log file entries during the reindex.

1. Select Start | All Programs | Microsoft SQL Server | SQL Server Management Studio.
2. Log on to SQL Server Management Studio.
3. Connect to the server running the database.
4. Open a new Query window.
5. Select the database.
   - The default name is Faultline.
6. Type exec dbo.fsDatabase_ReBuild_Indexes in the Query window.
7. Click Execute to execute the statement.

Monthly testing of backups
Once a month you should test your backups to ensure that you can restore your data in case of an emergency. If you don’t test your backups, you might find out they are not working as expected at the worst possible time – when you need them the most.

Each month, test a backup media from your off-site storage location and restore the databases to a test server. Make sure the database restores correctly.

Another test is to restore a sample database to your production server. If you are backing up the PUBS or NORTHWINDS databases that come with SQL Server, and have not deleted them, you can delete one from the SQL server and restore it from your backup media. If the database is restored, it is a good chance your Faultline database is also restorable.
Transaction log size

The default recovery model for the Faultline database is Full Recovery. With this model, if you do not periodically back up the transaction log, the file size can become very large when McAfee Vulnerability Manager runs for a long period of time.

The Full recovery model provides you with better flexibility for recovering databases to an earlier point in time. With Full Recovery model, you should include a transaction log backup in your backup plan.

- Back up your transaction logs. If you keep the recovery model set to Full Recovery, add the transaction log file to your regular backups.
- Shrink the database log. If you back up the transaction log file routinely and the log file size is still large, try to shrink the database by using the SQL Server Management Studio’s database shrink menu command. See the SQL documentation for more information at http://msdn.microsoft.com/en-us/library/ms189035.aspx.

If you don’t care about restoring the database to the exact point of failure in case of trouble, you can switch to the Simple Recovery model. See the SQL Server documentation for more information. With this model, the log file size remains small, and the database can still be recovered to the latest database back up.

Back up your transaction logs

Transaction logs are essential to the timely recovery of SQL Server databases.

1 Select Start | All Programs | Microsoft SQL Server | SQL Server Management Studio.
2 Log on to SQL Server Management Studio.
3 Right-click the Faultline database and choose Tasks | Back Up from the shortcut menu. The Back Up Database - Faultline window appears.
4 Type a name for the backup in the **Name** field and an optional description in the **Description** field.

5 To perform a transaction log backup, select **Transaction log** under **Backup type**.

6 Select a destination for the backup. This could be either an SQL Server backup device, tape, or a disk file. For example, select a disk file called D:\Backups\Faultline \Faultline_log.bak.

7 To view and, if necessary, modify the transaction log backup options, click the **Options** tab.
8 To remove any previous files with this name and create a new file, select **Overwrite Existing Media**.

9 Select your options, then click **OK**. A progress dialog box appears while the backup is being performed. When the backup is finished, a confirmation dialog box appears.

10 Click **OK**.

**Shrink the database**

McAfee does not recommend that you shrink the database on a regular basis because it could cause fragmentation. If you remove a lot of old data and you want to reuse the space, then you can shrink the database.

**Note:** You should be familiar enough with SQL to be able to run queries from the SQL Server Management Studio.

**View the current size of the database**

1 In the SQL Server Management Studio, run the following query to obtain the current file size

   ```sql
   data: sp_spaceused @updateusage = 'true'.
   ```

   This shows the file sizes in megabytes.

2 Note the size of the Faultline database, and the unallocated space.

**Calculate the optimal size**

The goal is to shrink the database so that it is a bit larger than the reserved space.
• Use the following equation to determine the percentage to shrink the database.
  \[
  \frac{\text{<target size>} - \text{<reserved size>}}{\text{<target size>}} = \text{Percentage to Change}
  \]

  Example:
  - Total database size = 30000 MB
  - Unallocated (free) space = 20000 MB
  - Reserved (actual) data size = 10000 MB
  - Target size = 15000 MB

  \[
  \frac{\text{15000} - \text{10000}}{\text{15000}} = 33\%
  \]

  This value is used in the following query to reduce the size of the database.

**Shrink the database using a query**

Use the following query by substituting the XX value with the percentage to be reduced.

```sql
USE Faultline
ALTER DATABASE faultline
SET RECOVERY SIMPLE
GO
CHECKPOINT
GO
DBCC SHRINKDATABASE ('faultline', XX)
GO
```

**Restore the database**

You can restore your database from a backup using SQL Server Management Studio.

1. Log on to the server running configuration manager.
2. Stop all scan engines using the configuration manager.
   a. Open configuration manager
   b. Expand the McAfee Vulnerability Manager tree in the left pane
   c. Select a scan engine and select **Stop**.
   You must do this for each scan engine.
3. Open SQL Server Management Studio.
   Select **Start | All Programs | Microsoft SQL Server | SQL Server Management Studio**.
4 Log on to SQL Server Management Studio.
5 Right-click the Faultline database and select Tasks | Restore | Database.
6 In the Restore Database - Faultline dialog box, type Faultline in the To database field.

You do not have to use Faultline as the database name. If you use a database name other than Faultline, you must add a string to the HKEY_LOCAL_MACHINE\SOFTWARE\Foundstone\Foundscan registry key in Windows 2003 or HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Foundstone\Foundscan registry key in Windows 2008 R2. The string must be DBName with the value of the name created for the McAfee Vulnerability Manager database.

If you use a database name other than Faultline, you should add the DBName registry key to any system that runs one or more of the following product applications or services:

- Scan controller
- Report engine
- Notification service
- Data synchronization service
- Configuration manager
- API server
Select **From device** and click the browse button.

In the **Specify Backup** dialog box, click **Add**.

Navigate to the location where the backup files are located, then click **OK**.

Click **OK** to exit the **Specify Backup** dialog box.

Under **Select the backup sets to restore**, select the database backup file.

If necessary, on the **Options** tab, you can edit the rows in the **Move to physical file name** column to specify the location and names of the physical files of the restored database.

Navigate to the location where the backup files are located, then click **OK**.

Click **OK** to exit the **Specify Backup** dialog box.

Under **Select the backup sets to restore**, select the database backup file.

If necessary, on the **Options** tab, you can edit the rows in the **Move to physical file name** column to specify the location and names of the physical files of the restored database.

Click **OK** to begin restoring the database.

When the restoring process is complete, a message appears. Click **OK** to close the message.

You can also restore the database by using a T-SQL script, which might reduce the manual work of changing the physical file locations. See "Restoring the database using T-SQL (page 119)."

Click **OK** to begin restoring the database.

When the restoring process is complete, a message appears. Click **OK** to close the message.

### Restore the database using T-SQL

You can restore your database from a backup using T-SQL.

You can also restore a McAfee Vulnerability Manager database by using T-SQL, which might reduce the manual work of changing the physical file locations in step 11 of the previous procedure.

Before running the script, you must set the values for three variables: @dbName, @backupFilePathName, and @DBFilePath.

- Use @dbName to specify the database name;
- Use @backupFilePathName to specify the database backup file name and location;
- Use @DBFilePath to specify the physical file location when the database is restored.

The T-SQL commands are as follows:

```sql
declare @SQLCommand nvarchar(4000)
declare @dbName nvarchar(50)
```
declare @backupFilePathName nvarchar(128)
declare @DBFilePath nvarchar(128)
set @dbName = N'[Faultline]'
set @backupFilePathName = N'D:\db.bak'
set @DBFilePath = N'D:\Database\Faultline\'
set @SQLCommand = 'RESTORE DATABASE ' +@dbName + ' FROM DISK =N''' + @backupFilePathName
+ ''' WITH  FILE = 1, NOUNLOAD , STATS = 10, RECOVERY , MOVE N''FaultlineAssets_01''
TO N'''
+ @DBFilePath + 'FaultlineAssets_01.ndf'',  MOVE N''FaultlineAssets_02'' TO N'''
+ @DBFilePath + 'FaultlineAssets_02.ndf'',  MOVE N''FaultlineAssets_03'' TO N'''
+ @DBFilePath + 'FaultlineAssets_03.ndf'',  MOVE N''FaultlineAssets_04'' TO N''
+ @DBFilePath + 'FaultlineAssets_04.ndf'',  MOVE N''FaultlineAssets_05'' TO N''
+ @DBFilePath + 'FaultlineAssets_05.ndf'',  MOVE N''FaultlineAssets_06'' TO N''
+ @DBFilePath + 'FaultlineAssets_06.ndf'',  MOVE N''FaultlineAssets_07'' TO N''
+ @DBFilePath + 'FaultlineAssets_07.ndf'',  MOVE N''FaultlineAssets_08'' TO N''
+ @DBFilePath + 'FaultlineAssets_08.ndf'',  MOVE N''FaultlineAssets_09'' TO N''
+ @DBFilePath + 'FaultlineAssets_09.ndf'',  MOVE N''FaultlineAssets_10'' TO N''
+ @DBFilePath + 'FaultlineAssets_10.ndf'',  MOVE N''FaultlineAssets_11'' TO N''
+ @DBFilePath + 'FaultlineAssets_11.ndf'',  MOVE N''FaultlineAssets_12'' TO N''
+ @DBFilePath + 'FaultlineAssets_12.ndf'',  MOVE N''Faultline'' TO N''
+ @DBFilePath + 'faultline.mdf''
+ @DBFilePath + 'faultline_log.ldf''
print @SQLCommand
exec(@SQLCommand)
GO

1 Open SQL Server Management Studio. To do this, select Start | All Programs | Microsoft SQL Server | SQL Server Management Studio.
2 Log on to SQL Server Management Studio.
3 Copy the T-SQL script above into a query window.
4 Set the values of the three variables: @dbName, @backupFilePathName, and @DBFilePath.
5 Run the script. To do this, select Query | Execute menu.

Note: You do not have to use “Faultline” as the database name. You can use a different name and add a registry string “DBName” under the registry key “HKEY_LOCAL_MACHINE\SOFTWARE\Foundstone\Foundscan” in Microsoft Windows 2003, or “HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Foundstone\Foundscan” in Microsoft Windows 2008 R2. Type the value of the product database name you specify in all the boxes that run a scan engine, report server, notification service, data synchronization service, API server, scan controller, or configuration manager.

Database index maintenance

A database index is used to improve the speed of retrieving data from a database. As McAfee Vulnerability Manager adds and removes asset information from the database index, the data might not be properly sorted and is no longer optimized to improve the speed of retrieving data.

The database index requires periodic maintenance for optimal performance. When scan data is written to the index and older scan jobs are removed, the index is not organized and can cause slower performance from your database. To assist users in maintaining their database index, the product provides an automated task. By default, this automated task is enabled.

The reorganization or rebuilding of table indexes is added as part of the database maintenance plan. When the task is enabled, it runs automatically every day. The results of the task are written to the FCServer.log file. You can check the FCServer.log file to see if the task actually reorganized or rebuilt the table indexes.
Maintaining the database
Regular maintenance for database integrity

- **INDEX REORGANIZATION**
  An index reorganization attempts to reorganize your database index to improve performance. This task can be performed while the database is in use (online). This task is similar to defragmenting a hard disk.
  This task specifies the index leaf level to reorganize. This clause is equivalent to `DBCC INDEXDEFRAG`. The `ALTER INDEX REORGANIZE` statement is always performed online. This means that long term blocking table locks are not held and queries or updates to the underlying table can continue during the `ALTER INDEX REORGANIZE` transaction.

- **INDEX REBUILD**
  An index rebuild saves a copy of your database index to a temporary location, the task then deletes all index entries and then replace all of your index entries in order. This task takes longer than an index reorganization and requires a lot of the server resources (cpu and memory).
  Perform this task during off-peak periods for your server. Performing this task when the server is busy can cause performance issues.
  This task specifies the index is rebuilt using the same columns, index type, uniqueness attribute, and sort order. This clause is equivalent to `DBCC DBREINDEX REBUILD`. `REBUILD` enables a disabled index. Rebuilding a clustered index does not rebuild the associated nonclustered indexes unless the keyword `ALL` is specified. If index options are not specified, the existing index option values stored in `sys.indexes` are applied. For any index option whose value is not stored in `sys.indexes`, the default indicated in the argument definition of the option applies.

- **ONLINE**
  In the task, ONLINE means the tables and indexes are available while the indexes are being rebuilt. This setting is either ON or OFF. By default, this setting is OFF. This setting is only available with the Microsoft SQL Server Enterprise Edition.

**Work flow**
- configuration manager starts the task by calling `[dbo].[fsMaintenanceSP_AlterIndexes]` with parameters specified in the `dbo.Maintenance` table.
- configuration manager receives the result message of the task and writes to the `FCServer.log` file.

**Modify the maintenance task**
This database index maintenance task is performed by using a stored procedure `[dbo].[fsMaintenanceSP_AlterIndexes]`. This procedure can reorganize or rebuild some of the table indexes in the database.

The procedure gets a list of fragmented tables and prioritizes them by criticality and fragmentation, then reorganizes or rebuilds the indexes of each table for a set amount of time.

The stored procedure updates the index statistics when it is complete.

1. Select **Start** | **All Programs** | **Microsoft SQL Server** | **SQL Server Management Studio**.
2. Log on to the database.
   You must have the SQL server authentication (user name and password) or Windows authentication to access the database.
3. Expand the **Databases** folder and select the **Faultline** database.
   If you changed the name of the database, select that database.
4. Click **New Query** and type the following:

   ```sql
   update dbo.Maintenance
   set FrequencyInDays=1, NextRunUTC='01/01/2009 00:00:00', P1='0', P2='30'
   where TaskID=70
   ```

   It is recommended that you use the default settings. If needed, the settings can be modified.

   - **FrequencyInDays=1** means the task runs every day.
   - **This sets the number days between automated task runs.** For example, changing this number to 7 would mean the task runs once a week.
Maintaining the database
Regular maintenance for database integrity

- NextRunUTC='01/01/2009 00:00:00' means the task starts at 12:00 AM (UTC time) each
time the task is run.
- P1 determines what the task does.
  P1='0' – The task reorganizes the table indexes for the amount of time set by parameter P2.
  P1='1' – The task checks for Microsoft SQL Enterprise Edition. If Microsoft SQL Enterprise Edition is
  installed, the task rebuilds any table indexes that do not contain any BLOB (binary large object) data
  columns. Any table indexes with a BLOB data column are reorganized. For non-Enterprise Edition
  installation (i.e. Microsoft SQL Standard Edition), only the table indexes are reorganized. The task runs for
  the amount of time set by parameter P2.
  P1='2' – The task rebuilds the table indexes for the amount of time set by parameter P2.
  P1='3' – The task rebuilds the table indexes until the task is complete. This setting ignores parameter P2.
- P2 is the number of minutes the database task is allowed to run, the default is 30 minutes.
  If you type zero or a negative number, the procedure runs forever.

5 Click Execute to enable this task.

Check the maintenance index results

After the database index maintenance task is complete, you can check the results by viewing the
FCServer log file.

1 Open the FCServer.log file.
   To open the FCServer log file, go to the server hosting the configuration manager, open the FCM
   folder (example: C:\Program Files\Foundstone\FCM), and locate the FCServer.log file.
   If database maintenance is enabled, you should see "Database Index Maintenance Message: Alter
   index task..." or a similar message in the log file.

2 The following is a list of possible messages, with descriptions:
   - Alter index task did not do anything – This means a few or none of the tables in the database
     were rebuilt. You should schedule a time to stop all McAfee Vulnerability Manager services and
     use the manual method to rebuild the indexes offline.
   - Alter index task made some progress, but did not finish – This means the task is able to
     rebuild some tables each time the task is run, but cannot rebuild all of the tables within 30
     minutes. This is acceptable behavior.
   - Alter index task completed – This means the task is able to rebuild all of the tables each time
     the task is run.

3 If you want to see the fragmentation of the indexes, you can manually run the following SQL
   query against the database in the Microsoft SQL Server Management Studio:
   a Select Start | All Programs | Microsoft SQL Server | SQL Server Management Studio.
   b Log on to SQL Server Management Studio.
   c Select the Faultline database.
   d Click New Query and type the following:
   
   ```sql
   select tblname = replace(replace((QUOTENAME(s.name) + '.' +
   QUOTENAME(o.name)),'[',''),'][','
   ,idxname = QUOTENAME(i.name)
   ,idx_type=i.[type]
   ,t.avg_fragmentation_in_percent
   ,t.page_count
   FROM sys.dm_db_index_physical_stats (DB_ID(), NULL, NULL, NULL, 'LIMITED') t
   join sys.objects o on t.object_id = o.object_id
   JOIN sys.schemas s ON s.schema_id = o.schema_id
   join sys.indexes i on t.object_id = i.object_id and t.index_id=i.index_id
   ```
   
   McAfee Vulnerability Manager 7.5 Product Guide 122
Click **Execute**.
The query runs and a table shows the results. The `avg_fragmentation_in_percent` column shows the percent of fragmentation for each table index. For a description on detecting fragmentation and how to interpret the results returned by the query, see the Detecting Fragmentation (http://technet.microsoft.com/en-us/library/ms189858(v=sql.90).aspx) on the Microsoft website.

**Note:** Rebuilding or reorganizing small indexes often does not reduce fragmentation.

### Disable the maintenance task

By default, the database index maintenance task is enabled. You can disable this task in the Configuration Manager.

#### Disable the task using the configuration manager

1. Open the configuration manager.
2. Select **Tools | Preferences**.
3. Select the **Database** tab.
4. Deselect the **Update Index Statistics** and **Index Defragmentation** checkboxes under **Recurring**.
5. Click **Apply**, then click **OK**.

#### Disable the task from the database server

1. Select **Start | All Programs | Microsoft SQL Server | SQL Server Management Studio**.
2. Log on to SQL Server Management Studio.
3. Expand the **Databases** folder and select the **Faultline** database.
   - If you changed the name of the database, select that database.
4. Click **New Query** and type the following:
   
   ```
   update dbo.Maintenance
   set FrequencyInDays=-1
   ```
5. Click **Execute** to enable the task.

### Manually run the maintenance index task

You can run the database index maintenance task manually. This allows you to run the task as needed, instead of waiting for the next scheduled run.

1. Select **Start | All Programs | Microsoft SQL Server | SQL Server Management Studio**.
2. Log on to SQL Server Management Studio.
3. Select the Faultline database.
4. Click **New Query**.
5. Type `exec fsMaintenanceSP_AlterIndexes '3', '0'`.
   - This SQL statement means to rebuild the database offline and to let the task run for as long as it takes to complete.
   - You should change the two parameters (‘3’ and ‘0’) based on your company’s guidelines or needs.
   - The first parameter determines what the task does. In the above example, this parameter is set to ‘3’.
     - ‘0’ – The task reorganizes the table indexes for the amount of time set by the second parameter.
'1' – The task checks for Microsoft SQL Enterprise Edition. If Microsoft SQL Enterprise Edition is installed, the task rebuilds any table indexes that do not contain any BLOB (binary large object) data columns. Any table indexes with a BLOB data column are reorganized. For non-Enterprise Edition installation (i.e. Microsoft SQL Standard Edition), only the table indexes are reorganized. The task runs for the amount of time set by parameter P2.

'2' – The task rebuilds the table indexes for the amount of time set by the second parameter.

'3' – The task rebuilds the table indexes until the task is complete. This setting ignores the second parameter.

- The second parameter is the number of minutes the database task is allowed to run. In the above example, this parameter is set to '0'.

If you type zero or a negative number, the procedure runs forever.

6 Click **Execute**.
Using the Configuration Manager

The configuration manager allows you to manage your McAfee Vulnerability Manager components. Using the configuration manager, you can manage component updates, SSL certificates, collect SSH target certificates, manage OS fingerprints, schedule maintenance tasks for the database, modify report server settings, modify some API server settings, and gather diagnostic information and log information.

When you install configuration manager, you install a configuration manager server and a configuration manager agent on the product system. When you install other product components on other McAfee Vulnerability Manager systems, the configuration manager agent is installed. The configuration manager manages communication using the configuration manager agent. The configuration manager agent is not required on systems accessing the enterprise manager using a web browser.

During installation of the product systems, default SSL certificates are installed and are used to authenticate communications between the various components (such as between the database and the scan controller or enterprise manager).

**Note:** If you want to use your own custom third-party certificates, use the McAfee Vulnerability Manager SSL Certificate Tool. This tool is available by contacting McAfee Technical Support.

Also note that you need to obtain this tool if you are using the McAfee Vulnerability Manager Open API.

Navigating the main window

The main window of the configuration manager contains a navigation tree, a details/information pane, and system status messages. Most actions you perform are accessed by selecting an item in the navigation tree.
In addition to the application window, the **Tools** menu includes items so you can change system preferences, recreate the Certificate Authority, manage OS fingerprints, show or hide automatically updated components (in the left node), and gather SSH server keys using configuration manager.

![Figure 31: FCM - Main Window](image)

**Main Window Descriptions**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Left pane. Contains nodes to expand/collapse or select.</td>
</tr>
</tbody>
</table>
| 2       | Details pane: Displays information on the node or item selected in the left pane.  

- **Advanced Actions**: Provides advanced settings for the configuration manager agent, disable automatic updates for the host, or initiate configuration manager tasks.  

| 3       | System message area: Displays messages and status of actions performed. Messages are color coded as follows:  

- Black - information  
- Red - error  
- Green - success  
- Purple - SSH collector error  
- Orange - warning  

- Click **Clear** to remove system messages. |

---

**How configuration manager systems are managed**

McAfee Vulnerability Manager is made of multiple components communicating with each other. The configuration manager allows you to manage that communication. The scan controller communicates with the database to transfer scanned system data to the database. The enterprise manager...
communicates with the database to gather the scanned data and present it in the web interface. If you installed all of the product components on a single, dedicated server (all-in-one deployment) there is no need to manage the communication between the components. If you installed the product components on two or more dedicated servers (distributed deployment), properly configuring communication between components is critical. The configuration manager assists in managing the communication between the product components.

Viewing systems with FCM agents

Some McAfee Vulnerability Manager components require a Configuration agent to help manage communication. The Configuration agent can also provide status information for the server running the product component.

1. On the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. In the configuration manager main window, in the left pane select the top node. The McAfee Vulnerability Manager Enterprise System List window appears in the right pane.
3. To sort any column, select the column heading. For example, to sort all trusted agents, select the Trusted column heading.

View system details

The configuration manager provides detailed information for each component running an FCM agent.

1. On the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. In the configuration manager main window, in the left pane, expand the Foundstone Systems node and then select the node for the system you want to view. The System details window appears in the right pane.
3. To manage this system, click the plus sign (+) to expand the Advanced Actions of the page. Use this section of the page to individually manage this host.
4. To prevent this system from receiving automatic updates, select the Disable automatic updates for this host checkbox. This checkbox is available only if the Global Update Policy is set to Automatic (this is set in the Preferences dialog box).
5. To start one of the advanced tasks, select it from the Tasks list, then select Initiate Task.
   - To stop all McAfee Vulnerability Manager components from running, select Stop All Components. This includes the scan engine, database, and so on. This action does not stop the Configuration server or Configuration agent.
   - To generate and install a customer-specific certificate on this system, select Issue Customer-Specific Certificate. The existing certificate is deleted from the system. When the product is installed, all components are installed with custom certificates. Use this option to generate customer-specific certificates using the Certificate Authority that is installed when configuration manager was installed.
   - To apply any update patches that have not yet been applied, select Apply All Packages. Use this option when the global update policy is manual, or when you have disabled automatic updates for this host.
   - To restart all components (and services) on this system, select Start All Components. This includes the scan engine, database, and so on.
   - To restart this system, select Reboot Host System.
   - To remove this system from the list of trusted (verified) hosts, select Revoke Trust. To establish secure two-way communications between components, including those UNIX-based devices using SSH certificates, the scan engine must be trusted.

Note: If the system is currently offline (if the Configuration agent is not connected to the Configuration server), only the Revoke Trust option is available.
Update configuration agent custom settings

Using custom Configuration Agent settings, you can specify the credentials for the agent to use when communicating with the database and change the settings for the McAfee Vulnerability Manager log files.

1. On the configuration manager server, select **Start | All Programs | Foundstone | FCM Console**.
2. Select a system under **Foundstone Systems**.
3. Expand **Advanced Actions**.
4. Click **Advanced Settings**.

![Custom Agent Settings](image)

Manually trusting FCM agents

When the configuration manager is installed, all FCM agents are automatically trusted. McAfee recommends that you keep this setting until all systems are online and functioning properly, then changing the system trust policy to manually trust agents. Any new systems added must be manually trusted.

1. On the configuration manager server, select **Start | All Programs | Foundstone | FCM Console**.
2. In the configuration manager main window, in the left pane, expand the **Foundstone Systems** node and then select the node for the system you want to trust. The System details appears in the right pane.
3. Click **Trust System**.

View component configurations

Component configuration information shows you the state of the component, the version details, and allows you to start or stop the component.
Assign scan engines to the scan controller

McAfee Vulnerability Manager uses a scan controller to manage multiple scan engines and provide communication with the database. The product allows you to have multiple scan controllers deployed.

The scan controller allows the product to have lightweight scan engines that can use simple HTTPS protocols, allowing scan engines to exist outside a firewall.

If you have one scan controller and you add a scan engine, the product automatically assigns the scan controller to the scan engine. If you have more than one scan controller, you can assign a scan engine to a scan controller.

1 On the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2 In the left pane, expand the scan engine information.
3 Select Scan Engine.
4 Select a scan controller from the Change Scan Controller list.
5 Click OK.

Configuration manager preferences

The product is made of different components and services that communicate with each other. Managing these communications is done using the configuration manager.

Each tab appears (Connected) or (Disconnected) in the upper-right-hand corner.

- (Connected) signifies that the component represented by the tab is connected to the database.
- (Disconnected) signifies that the component represented by the tab is not connected to the database.
  You should find the cause of the disconnection (e.g. need to start the server or database) and correct it.

Note: Changing preferences in the configuration manager while users are accessing the enterprise manager might cause some product functions to not work properly. Having users close and reopen their web portal session should resolve any issues.
Specifying FCM preferences

FCM preferences define how agents are trusted and configure the port used by the Configuration Manager component.

![Figure 33: FCM Preferences – FCM Tab](image)

Set the System Security Policy

Use the following task to change how McAfee Vulnerability Manager trusts configuration agents.

1. From the configuration manager server, select **Start | All Programs | Foundstone | FCM Console**.
2. Select **Tools | Preferences**.
3. Specify how you want to trust new agents that come online:
   - If you want to automatically trust all new agents, click the arrow and select **Trust all agents**.
   - The default settings automatically trust all new agents, but do not issue a certificate to them.
4. Click **Apply**.

**Tip:** McAfee recommends you keep these settings to automatically trust all new agents until all systems are up and running, then change the setting to manual trust verification. This allows you to quickly get all systems up and online, then review and approve any new agents that attempt to connect.

Set the Global Update Policy

Use the following task to specify how you want to update components.
1. From the configuration manager server, select **Start | All Programs | Foundstone | FCM Console**.

2. Select **Tools | Preferences**.

3. For **Package Application Timing**, select how you want updates applied to components and systems managed by this configuration manager server. This is known as the **Global Update Policy**.
   - To apply update packages automatically to any components as soon as the packages become available, select **Apply Automatically**. You can override this setting individually on each component (in the **System window**, expand **Advanced Actions** and select **Disable automatic updates for this host**).
   - To apply update packages manually, select **Apply manually**. To apply update packages to agents, in the System details window expand **Advanced Actions**. In the Task List, select **Apply All Packages** and click **Initiate Task**.

   When **Apply Automatic** is selected, all components are updated, including components set to manually update. For more information, see Updating Components (page 138).

4. Select **Send an email notification when an update is available/applied** checkbox to receive email notifications.

5. Click **Apply**.

*Note:* Be sure that the Global Administrator has enabled email notifications, and that a valid email address has been entered for **McAfee Vulnerability Manager Operations** (select **Manage | Notifications** in the enterprise manager).

---

**Set Configuration Manager port and interface options**

Use the following task to change port and interface for the configuration manager.

1. From the configuration manager server, select **Start | All Programs | Foundstone | FCM Console**.

2. Select **Tools | Preferences**.

3. To change the port that the configuration manager server listens on, type a new port for **Listening Port**. The default port is 3801.

   *Caution:* Don't change this setting while the configuration manager is busy performing other actions. or those actions will fail.

4. To change the network interface card (NIC) that the configuration manager server uses, for **Listening Interface** select the NIC from the list. Select **Any** to listen on any NIC, or select a specific NIC.

5. Click **Apply**.
Specify database preferences

If you change the database address or the database user logon, you must update the information on the Database preferences tab. You can also modify the database maintenance tasks on this tab.

Figure 34: FCM Preferences – Database Tab

1. From the configuration manager server, select **Start | All Programs | Foundstone | FCM Console**.

2. Select **Tools | Preferences**, then select the **Database** tab.

3. To change the connection to the database, do the following:
   
   a. For **Foundstone Database Address**, type the IP address, NetBIOS name, or fully-qualified domain name where the server is located.

   **Note**: While `<Server Name>,<port>` is a valid SQL server reference when using a named instance, this is not a valid reference for McAfee Vulnerability Manager. When using an instance name, the instance name must be included for the product to function properly. Example: `<Server Name><Instance Name>,<port>`. The port number might be optional, depending on your Microsoft SQL installation.

   b. If you are not using NT authentication, type a valid **Username** and **Password** to connect to the Faultline database. The default user name is Faultline. The password was created when the database was installed.
   
   You can also use the sa password.

4. To schedule database maintenance tasks, do the following:
   
   a. Enable a database maintenance task by selecting the **Recurring** checkbox.
   
   b. To schedule the number of days between running tasks, type the number of days in **Run this task every – day(s)**.
   
   c. To set the time of the scheduled task, specify a time in **Run this task every – at (time)**.

   The task runs at the selected time on the database. If your database is in a different time zone, the task runs based on the time zone of the database, not the configuration manager.
To run a task now, select Run Now, then select OK or Apply to run this task one time. This runs the task when the database is available. Using the Run now function does not require you to schedule a task.

For tasks with older than in the title, you can specify the number of days before the item is considered old and ready to be deleted.

**Note:** Scheduling database maintenance tasks affects all organizations associated with the selected database.

**Database maintenance task descriptions**

- **Delete inactive ePO Assets** – In McAfee Vulnerability Manager, rules can be created that determine when an asset becomes inactive. This task removes ePolicy Orchestrator assets that have been inactive longer than the selected number of days.

- **Update Index statistics** – Manually update the index statistics in the database. This silent process does not affect other users, but can increase the CPU usage on the database server.

- **Index Defragmentation** – Saves a copy of your database index to a temporary location, deletes all index entries, and replaces all of your index entries in order. This task takes longer than an index update and requires a lot of the server resources (cpu and memory). Perform this task during off-peak periods for your server.

  **Caution:** Performing this task when the server is busy can cause performance issues.

- **Archive Asset data** – Archives asset data older than one day.

  **Note:** For Archive Asset data, only the Run this task every – at (time) field and Run Now are selectable options. The frequency of archiving asset data is set to assist in database maintenance.

- **Delete jobs and stale tickets older than** – Clears out old jobs and stale remediation tickets after the number of days that you specify. If the state of a ticket is closed, complete, auto-closed, false-positive, false-positive-acknowledge, or ignored, it is deleted after the number of days you specify. If the product discovers the same vulnerability on the host after this ticket has already deleted, it opens a new ticket for that vulnerability.

- **Delete historical Asset data older than** – Deletes archived asset data older than the selected number of days.

- **Delete Events and Errors older than** – Removes entries from the event history file and entries from the error table (in the database) that are older than the selected number of days. These entries can consume a large amount of hard disk space if not maintained.
Specify report server preferences

To make changes to the Report Server settings (such as the number of reports that can be generated at the same time), use the Report Server preferences tab.

1. From the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. Select Tools | Preferences, then select the Report Server tab.
3. To increase (or decrease) the number of concurrent reports allowed during report generation, change the number in the Maximum concurrent reports field.
4. To increase (or decrease) the file size allowed for an email attachment, change the number in the Maximum attachment size (MB) field.
5. To modify the HTTP Server settings:
   a. To change the listening port, change the port number in the Listening Port field. Modifying the port while users are logged on to the web portal might cause some McAfee Vulnerability Manager functions to not work properly. Having users log out and log back on should resolve this issue.
   b. To enable SSL, select Use SSL. If you enable SSL, you also have the option of requiring client authentication.
6. To modify the report settings for Enterprise Manager:
   a. Select Enable Pushing Reports to Enterprise Manager.
   b. Type the enterprise manager server address in the Server Address field.
   c. To enable SSL, select Use SSL. If you enable SSL, you also have the option of requiring authentication.
   d. To use a custom port, select Use custom HTTP/HTTPS port. Type the custom port number in the port field.
   e. To automatically delete reports once they have been delivered, select Delete report files from Report Server after delivery.
7. To copy reports to a network drive:
   a. Select Copy Reports to Network Drive.
Specify report server service settings

The report server settings define the maximum number of concurrent reports to generate, maximum email attachment size, and other report server settings.

1. Select **Start | Administrative Tools | Services.**
2. Right-click **Foundstone Report Server** and select **Properties.**
3. Select the **Log On** tab.
4. Select **This Account.**
5. Type the user name and password. This information must be for a valid user who has the appropriate permissions to share files on this host.
6. Click **OK.**
7. Restart the **Foundstone Report Server** service.

Specify API server settings

Use the API Server preferences tab to modify the communication settings between the API server and the web portal.

![Figure 36: FCM Preferences – API Server tab](image)
When you make changes, you must restart API server for McAfee Vulnerability Manager to use the new setting.

Caution: Don’t change the SSL settings without configuring the enterprise manager to match your selection. Otherwise, the enterprise manager and configuration manager can’t communicate.

Selecting Incoming Connection options

Use the following task to change the API server connection settings to listen for communications coming from the enterprise manager.

1. From the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. Select Tools | Preferences, then select the API Server tab.
   • Use custom port – Select this to specify port settings. Type the port number that the API server uses to receive product information. The default port setting is 3800.

Note: Using a custom port requires modifying the api_primary setting in the enterprise manager config.ini file.

• Use SSL (secure protocol) – Provides secure communication between the API server and the enterprise manager.

Note: If you use SSL, your IIS server must contain a valid SSL Certificate.

• Use custom session timeout (in minutes) – Select this to specify the number of minutes of inactivity allowed before the session is disconnected.

3. Click Apply.

Note: Applying a change to the custom session timeout ends the session for any logged on users. When users attempt to modify something or navigate to another page, they are notified that they are logged off. Users must log on again.

Selecting Enterprise Manager communication options

Use the following task to change the API server connection settings to push information to the enterprise manager (including asset search results and status messages).

1. From the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. Select Tools | Preferences, then select the API Server tab.
   • Enterprise Manager Server address – Type the IP address, DNS name, or NetBIOS name for the web server running the enterprise manager.
     If you change the enterprise manager server Address, you must change the config.ini file on the computer hosting the enterprise manager. On the enterprise manager, the path to the config.ini file is Foundstone\Portal\include. Change server_name, under [server], to match the address on the API Server tab.
     If you leave the address blank, reports are not available through the enterprise manager (unless it is running on this system, which is not recommended).
   • Use custom port – Select this to specify port settings. Type the port number that the enterprise manager uses to receive McAfee information. The default port setting is 443.

Note: This number must match the port that the enterprise manager uses.

• Use SSL (secure protocol) – Provides secure communication between the enterprise manager and the API server.

Note: If you use SSL, your IIS server must contain a valid SSL Certificate.

3. Click Apply.
Specify External Interface settings

If you use a firewall or load balancer, McAfee Vulnerability Manager allows communication between a scan engine and a scan controller through a firewall or load balancer.

You must configure your firewall or load balancer to allow communication between the scan engine and scan controller. If the port number for the external interface must be changed, create a new External Interface with the new port number and then update the product components to communicate with the new External Interface.

1. From the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. Select Tools | Preferences, then select the External Interfaces tab.
3. Select Enable External Interface communication.
   As an added measure of security, the scan controller identifies a scan engine. If the scan controller cannot identify the scan engine, communication is not allowed. Connecting a scan engine through a firewall or load balancer breaks this identification process. You must disable this process when using a scan controller and scan engine separated by a firewall or load balancer.
4. Click Add.
5. Type a unique name for the proxy.
6. Double-click the IP address field and type the IP address for the firewall or load balancer.
7. Double-click the port field and type the port number the firewall or load balancer is listening on.
8. Click OK.

Specify scan controller preferences

The Max Database Connection Pool value is the maximum number of concurrent connections a scan controller can make to the database. If the server running your database exceeds the minimum system requirements, you can adjust this number to improve product performance.

1. In the configuration manager, select Tools | Preferences.
2. Select the Scan Controller tab.
3. Type the maximum number of connections allowed for all connected scan controllers. If a scan controller is offline, this change does not affect that scan controller.

   **Note:** Zero is not a valid number for the Max Database Connection Pool.

4. Click Apply.

Specify scan engine preferences

You can set the maximum amount of time allowed for a response to a post operation before it is timed out by the scan engine. There is an initial timeout value and two retry timeout values.

1. In the configuration manager, select Tools | Preferences.
2. Select the Scan Engine tab.
3. Type a value for the Initial timeout, First retry, and Second retry. The values must be between 1 and 600. The First retry timeout must be greater than the initial timeout, and the Second retry timeout must be greater than the First retry timeout.
4. Click Apply.
How configuration manager updates components

The configuration manager manages two types of components: those that can be manually or automatically updated, and those that are always automatically updated. You can modify this setting in the Preferences dialog box.

Note: All automatic or manual components are listed in the left pane of the configuration manager when you have expanded a McAfee Vulnerability Manager system. Select to view or hide components that are always updated automatically by selecting Tools | Show AutoUpdated Components.

Components that can be updated automatically or manually
- Data synchronization service
- Scan engine
- Scan controller
- FASL engine
- Faultline database
- API server
- Configuration agent (FCM)
- Configuration server (FCM)
- FSUpdate
- Notification services
- Enterprise manager
- Report server
- MVM 3000
- MVM 3100

Components that are always updated automatically
- All languages, including English, Japanese, Spanish, German, French, Korean, Chinese Simplified, Chinese Traditional
- OS Prints
- Custom OS Prints
- FASL scripts

How OS fingerprints work

If McAfee Vulnerability Manager cannot identify the operating system, the system is listed in the Identify Operating System dialog box. You can manually add that information so the product can properly identify the system in the future.

Update OS fingerprints

Use the following task to manually add OS fingerprint information.

1. From the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. Select Tools | Manage OS Fingerprint.
3. To update an IP address once you know its operating system, find the IP address in the list and double-click it. This opens the Identify Systems dialog box.
4 Type the new information and click OK.

![Figure 37: Update your OS fingerprint to identify unknown operating systems](image)

**Identify systems**

When you specify the operating system information, each time McAfee Vulnerability Manager discovers this system or another system with the same OS fingerprint, the specified information is used to identify the operating system.

This information is saved in the CustomOSPrints file on this scan engine, and the database is updated. The next time a scan identifies this host, it uses the new Operating System and description.

- To update the host information, select the operating system from the Operating System field, and type a description.

**How SSL certificates work**

Certificates are sets of electronic files, created by a trusted Certificate Authority. The certificates allow systems to authenticate to each other, thereby trusting them to receive confidential information using encrypted communication.

SSL certificates contain the following information:

- Your organization's common name (for example, [www.mcafee.com](http://www.mcafee.com))
- Additional identifying information (IP address and physical address)
- Your public key
- Expiration date of the public key
- Name of the CA that issued the ID (such as VeriSign)
- A unique serial number

The certificate is digitally signed with the Certificate Authority's private key. So if you trust the CA, and you have the CA's public key, you can verify and be assured of the certificate's legitimacy.

The configuration manager is designed to enable SSL (X.509) server-certificate creation, as well as the secure distribution and installation of those certificates. Server certificates contain public and
private keys used by a McAfee Vulnerability Manager system component. The private key is the crucial element in the authentication process and must be kept secure.

The product consists of four main components: The database, enterprise manager, API server, and scan controller. To run in a secure environment, communications between these components must be encrypted.

### Issue certificates to components

When McAfee Vulnerability Manager is installed, all components are installed using a custom certificate. To change to a customer-specific certificate, you need to reissue certificates to each FCM agent.

1. On the configuration manager server, select **Start | All Programs | Foundstone | FCM Console**.
2. Expand the node in the left pane for the system you want to issue certificates for.
3. In the **System details** window, click the plus sign to expand the **Advanced Actions**.
4. In the Task List, select **Reinstall Customer-Specific Certificate**.
5. Click **Initiate Task**. Messages appear in the status bar when certificates have been installed on the product components installed on that system.

### View certificate details

The certificate details include summaries of the system (Assigned Host), certificate, the issuer (Certificate Authority), and the public certificate.

The certificates listed in the left pane of the window also include the public certificate for the Certificate Authority. View the details of this certificate just as you would an agent’s details.

![Figure 38: FCM – Certificate window](image)
Using the Configuration Manager
How SSL certificates work

1. On the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. In the left pane, expand the Foundstone SSL Certificates node and select the certificate you want to view.
   The Certificate information appears in the right pane.

Recreate the certificate authority

When the configuration manager is installed, a Certificate Authority (CA) is created. If necessary, you can recreate the Certificate Authority.

Creating a new CA deletes the current CA and all certificates are invalidated. Communications between the McAfee Vulnerability Manager components continue to use the old certificates until the new certificates are installed. McAfee strongly recommends that you stop all components before recreating the CA, then install new certificates.

1. On the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. It is recommended that you reset the system trust policy to manual, especially if you suspect there is an issue with a compromised product system in your deployment.
   To change your system trust policy to manual, select Tools | Preferences, and select the FCM tab. In the Preferences dialog box, for Agent Trust Policy, click the arrow and select Manual Trust Verification.

4. Type a name for the CA. The name cannot exceed 64 characters and can include any characters except for: comma, plus sign, double quotes, single quotes, semicolon, less than symbol, greater than symbol, leading pound sign, and leading space.
5. Click Recreate Certificate Authority. The CA is recreated.
6. Manually trust each system and issue new certificates to each one (if you have not selected to automatically issue certificates to trusted systems).
View customer-specific certificates

The McAfee Vulnerability Manager Certificate Store is a list of customer-specific certificates currently installed on the systems managed by the Configuration Manager server.

The information on the certificates listed in this window include the Agent IP, resolved host name and FQDN, the common name of the public key, the type of key and length, and the start and end dates of the key.

1. On the configuration manager server, select Start | All Programs | Foundstone | FCM Console.
2. Select the Foundstone SSL Certificates node in the left pane.
   The Foundstone Certificate Store window appears in the right pane.
Troubleshooting

This section provides information on common questions and issues.

Scan engine is missing from the Manage | Engines list

The Manage | Engines page shows the available engines, but one or more engines do not appear.

Problem
The engines are not available to your organization or workgroup.

Solution
1. Log on as the Global Administrator.
2. In the organization or workgroup properties, go to the engines tab and make sure that the engines are available to your organization or workgroup.

Uploading reports does not work

A report doesn’t get uploaded to the McAfee Vulnerability Manager web portal, but other reports seem fine.

Problem
An application on your network might be limiting the files that get passed through by their size. By default, the product breaks the reports into 1MB file segments. Any program that limits files to 1MB or smaller might be preventing reports from properly uploading.

Solution
Check your network for any application that filters files according to their size.

- Check the IIS settings to see if you have set up ISAPI filters. If you are, remove the filter or edit its settings and see if the problem is resolved.
- Are you using URLScan on your network? URLScan can limit the size of files that can be uploaded to the enterprise manager. You might need to change the setting in the URLSCAN.INI file. The setting MaxAllowedContentLength=1000000 is set to 1MB by default. Raise this limit to 2MB (2000000) to allow reports to be uploaded from the report engine to the enterprise manager.

Updated the custom HTTP/HTTPS port, now report generation fails

You updated the custom HTTP/HTTPS port in the configuration manager Preferences dialog box and now your report generation is failing.

Problem
The SSL port number in the Internet Information Services (IIS) Manager on the host running the report server must match the custom port specified in the configuration manager.
**Solution**

Change the SSL port number in the IIS Manager on the host running the report server.

1. Select **Start** | **Administrative Tools** | **Internet Information Services (IIS) Manager**. The **Internet Information Services (IIS) Manager** window appears.
2. Expand the IIS tree and select the web server you want.
3. Expand **Web Sites** under the server you want.
4. Right-click the website you want to update and select **Properties**.
5. Change the **SSL port** to the port number specified in the configuration manager.
6. Click **OK**.

**A Linux target shows up as an Individual Host when it is part of a domain**

If you used the Shell Advanced Scan template to create a report and a Linux target is showing up in the report as an Individual Host, even though it is part of the scanned domain, could be caused by SAMBA share being disabled on the target.

To view the credentials being reported as part of the domain, SAMBA share on the Linux target must be enabled.

The shell module attempts to use a domain credential to log on to a host, even if that host is not on the domain. The module found the host, it found the domain, but no individual host credentials worked. The shell then tries to log on using the domain credentials as a foreign domain. That succeeds, but the host is not in the domain, so it is an individual host logging on using a foreign domain credential.

**How to use Active Directory/LDAP in the product**

The settings for an Active Directory or LDAP data source in McAfee Vulnerability Manager require specific settings that causes issues if configured improperly.

**Using Generic, NTLM, or Simple authentication**

For synchronization with Active Directory, use Generic or NTLM authentication. If you use NTLM, you must provide a domain name.

Simple authentication should be used with an OpenLDAP server. Simple authentication uses a plain, unencrypted user name and password. Simple authentication requires the user name to follow the format `cn=User,ou=People,o=Company`.

For example: `cn=Manager,dc=foundstone,dc=com`

**Search Root examples**

LDAP Search Root is the root of a domain (Active Directory), for example: `dc=foundstone,dc=com`.

There is a free tool called Softerra LDAP Browser which allows you to connect to the Active Directory and browse it. This tool can be downloaded from: [http://www.ldapadministrator.com/download.htm](http://www.ldapadministrator.com/download.htm).
To use this tool, you must provide the following information:

- The Base Domain Name, for example: dc=foundstone,dc=com
- Bind using the appropriate credentials to the Active Directory
- The Filter. For example: objectclass=computer brings all computer assets from the computer entry.

**SSL support**

The Active Directory administrator would be able to tell you if the directory supports SSL or not. The Active Directory needs to be configured specifically to enable LDAP over SSL. A fully-qualified domain name (FQDN) is required if you are using an SSL connection.

**Examples of search filters**

The LDAP search filters enable you to define search criteria and provide more efficient and effective searches. You must include parentheses () around the search filter. Leaving the parentheses off causes errors.

- (objectclass=*)
  You can use the wildcard operator in the filter to represent a value that could be equal to anything. This search returns every entry from the Active Directory.
- (objectclass=computer)
  This search returns all computer assets from the computer entry.
- (&(objectclass=computer)(!cn=Computer1))
  This search returns all computers except for Computer1.
- (&(objectclass=computer)\(\(|\left(cn=A^*\right)\left(cn=B^*\right)\left(cn=C^*\right)\left(cn=D^*\right)\left(cn=E^*\right)\left(cn=F^*\right)\))
  This search returns all computers with a name starting with A, B, C, D, E, or F.

**Standard values for Active Directory attributes**

There is no standard value for any of the Active Directory attributes. The table below lists possible values, but each Active Directory administrator can configure the attributes differently, as long as it meets the schema definition. For example, the administrator could use a value name instead of nETBIOSName as the NETBIOS-Name attribute. So the best way to find the attributes is to use the LDAP browser to look for them, or contact the Active Directory administrator.

<table>
<thead>
<tr>
<th>Attribute Common Name</th>
<th>Possible LDAP Display Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NETBIOS-Name</td>
<td>nETBIOSName or name</td>
<td>Name of the object used over NetBIOS.</td>
</tr>
<tr>
<td>DNS-Host</td>
<td>dNSHostName</td>
<td>The DNS or host name.</td>
</tr>
<tr>
<td>Network-Address</td>
<td>networkAddress or ipaddress</td>
<td>TCP/IP address for a network segment. Also called the subnet address.</td>
</tr>
</tbody>
</table>

**How an IP address resolved using NetBIOS and DNS attributes**

Standard Winsock methods are used to look up the IP address for a given hostname.
View or troubleshoot retrieved data

If you were successful in creating your LDAP data source and the last synchronization status shows a success, you can view or troubleshoot the retrieved data. You can access the Active Directory objects on the Targets tab of the scan wizard by selecting **Browse** and selecting the LDAP data source from the **Asset Source** list.

LDAP data sync shows success, but assets are not showing up

If McAfee Vulnerability Manager shows your LDAP synchronization as successful but the assets are not showing up when configuring a scan, there are two possibilities.

1. Search the LDAP Assets table in the database. If you don't see any assets in the table for the given LDAP data source, most likely that data synchronization didn't find any assets based on your search criteria (defined in the data source configuration). Make sure the search root, search filter, and attribute values are correct.

2. If you see the assets in the LDAP Asset table, check the IP pool of the user's root organization. If the IP addresses of individual LDAP assets are not in the range of the IP pool, the assets aren't added to the scan configuration editor.

Links to Active Directory documents about LDAP query basics

The following links are for Microsoft Active Directory documents describing LDAP query basics.


Unable to view Benchmark Scan reports in the enterprise manager

The scan status for a Benchmark Scan shows as Failed or after a benchmark scan is complete, the report is not available through the McAfee Vulnerability Manager web portal.

**Problem**

If you are unable to view your XCCDF/OVAL reports from the enterprise manager, your report might be too large for the product to post to the Enterprise Manager for viewing.

This can also cause a Failed status to appear on the scan status page.

**Solution**

- If the scan completed, but the report is not available through the enterprise manager, you can retrieve the report from the Report Server and manually uncompress the file.
- You can run a smaller scan to generate a smaller report. For scan configurations, scan for a smaller group of assets. For custom reports, adjust the asset filter to report on fewer assets.
- For a Failed scan status, check the Report Server log file. If the log file states that the transferring of the report to the enterprise manager failed, you can get the report from the Report Server and manually uncompress the file.
# Index

## A
- access ........................................................................ 23
- activity logs ................................................................ 24
- administrators .......................................................... 23
- assets ........................................................................ 36, 40
  - asset properties ...................................................... 40
  - asset tags ............................................................... 42
  - assets, criticality levels ......................................... 40
  - assets, viewing ...................................................... 40
- assignment rules, automatic ....................................... 96
- auto-close tickets ..................................................... 95

## C
- credential sets .......................................................... 59

## D
- due dates, remediation tickets ..................................... 95

## E
- engines ................................................................. 26
  - engines, setting properties of .................................. 26

## G
- global
  - global remediation settings .................................... 95
- Global Administrator ......................................................... 23

## H
- How scans work ........................................................ 56

## L
- LDAP ........................................................................ 28
- logging ...................................................................... 24
- logs, activity ............................................................. 24

## M
- menus ....................................................................... 100

## O
- organizations
  - organization administrator ......................................... 23
  - OVAL ....................................................................... 74

## P
- properties
  - properties, of assets ........................................... See asset properties
  - properties, setting engine ......................................... 26

## R
- read-only vulnerability set ........................................ 68
- remediation
  - remediation administrator ........................................ 23
  - remediation options ............................................... 95
  - remediation rules ................................................... 96
- role-based access ...................................................... 23
- rules, remediation ...................................................... 96

## S
- scan details .............................................................. 53
- searching
  - searching, for assets ............................................ 37

## T
- Tags, assets ................................................................ 42
- threats ..................................................................... 100, 101
- Threats menu .......................................................... 100
- toolbars .................................................................... 37

## U
- ungrouped assets ...................................................... 40
- users ....................................................................... 23

## V
- viewing
  - viewing, activity logs ............................................ 24
- vulnerability set, read-only ......................................... 68
- vulnerability sets ...................................................... 63

## W
- workgroups, working with
  - workgroups, administrator ....................................... 23
X

XCCDF ................................................................. 76