About this document

Thank you for using McAfee® Vulnerability Manager® 7.5.0 software. This document contains important information about this release. We strongly recommend that you read the entire document.

NOTE: McAfee Vulnerability Manager (MVM) was known as Foundstone.

CAUTION: We do not support automatic upgrading of a pre-release version of the software. To upgrade to a production release of the software, you must first uninstall the existing version of the software.

New features

New and updated features in the current release of the software are described below:
Vulnerability Manager dashboards

Vulnerability Manager has a new dashboard containing summary information about vulnerabilities, operating systems, and trend graph.

The new dashboard information includes:

- Most Prevalent Vulnerabilities – Displays 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.

- Most Prevalent Operating Systems – Displays 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.

- Vulnerability Count by Severity – Displays the number of High, Medium, Low, and Information vulnerabilities. This chart is updated once every 24 hours. Clicking on a severity level displays the Vulnerabilities by Severity page, with the severity level information expanded.

- Vulnerability Count by Percentage – Displays the percentage of High, Medium, Low, and Information vulnerabilities. This chart is updated once every 24 hours. Clicking on a severity level displays the Vulnerabilities by Severity page, with the severity level information expanded.

- Organization Vulnerability Count Trend – Displays a trend graph of the High, Medium, Low, and Information vulnerabilities for the organization, over time. This chart is updated once every 24 hours. 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. Clicking View Foundscores displays a trend graph based on the Foundscore.

  **NOTE:** Workgroups might see a difference between their vulnerability count and the trend graph. The vulnerabilities are for their workgroup, but the trend graph is for the organization the workgroup belongs to.

IPv6 scanning

Vulnerability Manager allows scanning of Internet Protocol version 6 (IPv6) addresses.

Enter your IPv6 addresses as you would your IPv4 addresses. You can type in each address, type in an IP range, or you can import your addresses and ranges from a file.

Vulnerability Manager allows you to omit leading zeroes and replace groups of consecutive zeroes with a double colon.


When including IPv6 address ranges in a file, separate the starting and ending addresses with a hyphen.

- Example: fe80::202:b3ff:fe1e:8329 - fe80::202:b3ff:fe1e:8400

  **NOTE:** If you are upgrading from a previous version, you must update your IP pool to include IPv6 ranges.

Scan details page

The scan details show the progress of different processing during a scan. This includes information during the discovery, assessment, and post-processing phases of a scan. This information provides more details on how the scan is progressing.

  **NOTE:** Some scan types perform assessment but do not scan for vulnerabilities. These scans will 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 <product> Policy Auditor Data Collection scan.

Asset tags and organizing assets

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

Vulnerability sets
Create a vulnerability set to target which vulnerabilities to scan for and generate reports for.

The product also provides some predefined vulnerability sets based on popular compliance standards, like the latest Microsoft patches, CWE/SANS Top 25, and OWASP Top 10. These are known as McAfee Vulnerability Sets.

**SUDO scanning**
The product allows users to use SUDO instead of SU for running individual commands in privileged mode.

**Notifications for scan and engine related events**
Three new scan email notifications and one scan engine email notification have been added to the product.

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

- Engine offline – An email notification is sent when a scan engine goes offline.

**Ports in reports**
For general vulnerabilities and web FSL checks, the port number, service, and protocol are now included in the Vulnerability Details and Vulnerabilities by IP report sections.

**Configuration manager preferences**
The configuration manager has two new tasks and two new Preferences tabs.

- Gather diagnostic info and logs task – Gathers log files and other information to assist in troubleshooting by customer support. These files may include the enterprise manager configuration file, product configuration files, and log files.

- Apply registry tweaks task – Applies registry tweaks from an XML file. This is not a global task; you must initiate this task for each system you want to apply the registry tweaks to.

  **NOTE:** This feature will be hidden by default when the product is released.

- Scan controller preferences tab – Sets the maximum number of concurrent connections a scan controller can make to the database.

- Scan engine preferences tab – Sets the maximum amount of time allowed for a post operation to get a response before it is timed out by the scan engine.

**Microsoft Windows Server 2003 support**
The product supports Microsoft Windows Server 2003 for the scan controller and scan engine only, with some limitations.

- No support for Internet Protocol version 6 (IPv6) scanning.
- No support for McAfee ePolicy Orchestrator or McAfee Policy Auditor integration.
- No support for McAfee Network Security Manager (NSM) integration.

**Known issues**
For a list of known issues for this release, see the following KnowledgeBase article:

- [KB75422](#)
Resolved issues
Issues from previous releases of the software that are resolved in this release are listed below.

Installation and upgrade

• **Issue**
  Installation fails when trying to install the McAfee Vulnerability Manager database on a system running .NET 4.0. (589403)

  **Resolution**
  Remove NET 4.0 before installing McAfee Vulnerability Manager. This is documented in the McAfee Vulnerability Manager Install Guide.

• **Issue**
  After an upgrade, verify that any custom port settings are properly configured. (566910, 556664)

  **Resolution**
  Custom port settings are maintained when upgrading McAfee Vulnerability Manager.

• **Issue**
  When installing the scan controller as the only component on a system, typing in a custom port number does not work and the default port is used. (558157)

  **Resolution**
  Custom ports work when installing the scan controller as the only component on a system.

• **Issue**
  When adding components, like a scan engine or scan controller, make sure the time on all systems are correct. If the time is not correct, SSL certificates might be out of synchronization and components might not connect properly. (580831)

  **Resolution**
  Product components connect even when the time is out of synchronization.

Scan and scan configuration

• **Issue**
  When removing Informational Crawl-Only vulnerabilities from an Informational Web Crawl scan configuration, the web application vulnerabilities are listed in different vulnerability categories. So deselecting the web application vulnerability in one category does not remove it from the scan configuration. To remove a web application vulnerability from a scan configuration you must deselect it from all categories before saving the scan configuration. (589747)

  **Resolution**
  Added this information to the product online help.

• **Issue**
  When creating a web application scan configuration, selecting a credential set and manually typing credentials might result in only some of the credential names appearing in the **User Credentials Used** section of the report. (589780)

  **Resolution**
  Now all credential names appear in the report.

• **Issue**
  When using form authentication in a web application scan, form authentication might be applied to any page with a form, not just the pages assigned in the scan configuration. (588696)

  **Resolution**
Form authentication in a web application scan functions properly.

- **Issue**
  When running a scan with Perform SSH Key Collection enabled, the scan status is not properly updated. The scan status might remain at zero for the duration of the scan and then update to 100%. (586629)

  **Resolution**
  The scan status updates properly.

- **Issue**
  If the organization administrator tries to create a new scan by right-clicking in the **Name/Description** pane (right pane) of the **Users/Groups** page, an error message displays stating the user does not have sufficient access rights to create a scan. Create a new scan by right-clicking in the organization tree (left pane). (587306)

  **Resolution**
  New scans are created when right-clicking in the **Name/Description** pane (right pane) of the **Users/Groups** page.

**Reports**

- **Issue**
  If you receive a report generation fail message when creating a large report, the issue could be with the upload limit in IIS 7.5. By default, IIS 7.5 limits the upload to 30 MB. When installing McAfee Vulnerability Manager, this limit should be increased to 300 MB. In some installation scenarios, the larger upload limit is not set. If your reports are not appearing in the enterprise manager after the scan completes, you can either retrieve the compressed report files from the report server or you can manually increase the IIS 7.5 upload limit. (580626, 589314)

  **Resolution**
  The report properly appears in the enterprise manager.

- **Issue**
  When generating large reports with all report types selected (CSV, HTML, PDF, and XML), the reports might be too large to post to the enterprise manager. If your reports are not appearing in the enterprise manager after the scan completes, retrieve the compressed report files from the report server. (589314)

  **Resolution**
  The report properly appears in the enterprise manager.

**Enterprise manager**

- **Issue**
  The workgroup administrator cannot see web application configurations in use from a configuration created by the organization administrator. When an organization administrator creates a web application configuration and makes it available to workgroup administrators, the assets or scan configurations associated with this web application configuration are not visible to the workgroup administrators. Only the organization administrator can view which assets and scan configurations are associated with the web application configuration, since multiple workgroups could be using it, and that information should not be accessible to other workgroups. (589931)

  **Resolution**
  Workgroup administrators can see the web application configurations in use from a configuration created by the organization administrator.

- **Issue**
  Trying to remove an asset from a group using the Remove from Group feature might not work. If the Remove from Group feature does not work, then move the asset to the root organization. (590250)

  **Resolution**
  The Remove from Group feature now functions properly.
• Issue
When trying to create a group with an existing name, the new group is not created and no message displays that the name is already in use. (580879)

Resolution
An error message displays that the group name is already in use.

Scan engine and scan controller
• Issue
The scan controller is a new component for McAfee Vulnerability Manager 7.0. If you are upgrading and a Scan Engine cannot communicate with any Scan Controller warning message appears in the configuration manager, you must manually assign a scan controller to the scan engine. (589928)

Resolution
Scan engines are assigned to a scan controller during an upgrade.

• Issue
When the global administrator assigns a scan engine to an organization, the scan engine also appears in the workgroups. The organization administrators must make sure the scan engine is properly assigned within their organization. (587688)

Resolution
Added this information to the product online help.

Ticketing and notification issues
• Issue
When email notifications are enabled for the organization administrator, the scan started email notification might not display the IP range. (589932)

Resolution
The scan started email notification displays the IP range.

Where to find McAfee enterprise product information
The McAfee documentation is designed to provide you with the information you need during each phase of product implementation, from evaluating a new product to maintaining existing ones. Depending on the product, additional documents might be available. After a product is released additional information regarding the product is entered into the online Knowledgebase available on McAfee ServicePortal.

<table>
<thead>
<tr>
<th>Evaluation Phase</th>
<th>Installation Phase</th>
<th>Setup Phase</th>
<th>Maintenance Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>How can my company benefit from this product?</td>
<td>Before, during, and after installation.</td>
<td>Getting up-and-running with the product.</td>
<td>Maintaining the software.</td>
</tr>
<tr>
<td>Evaluation Tutorial</td>
<td>Release Notes</td>
<td>Product Guide and Online Help</td>
<td>Online Help</td>
</tr>
<tr>
<td>Preparing for, installing and deploying software in a test environment.</td>
<td>Known issues in the current release.</td>
<td>Setting up and customizing the software for your environment.</td>
<td>Maintaining the software.</td>
</tr>
<tr>
<td>Detailed instructions for common tasks.</td>
<td>Issues resolved since the last release.</td>
<td>Online Help</td>
<td>Reference information.</td>
</tr>
<tr>
<td>Installation Guide</td>
<td>Last-minute changes to the product or its documentation.</td>
<td>Managing and deploying products through ePolicy Orchestrator.</td>
<td>All information found in the product guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Detailed information about options in the product.</td>
<td>Quick Reference Card</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Detailed instructions for common and infrequent important tasks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Knowledgebase (knowledge.mcafee.com)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Release notes and</td>
</tr>
</tbody>
</table>
Finding release notes and documentation for McAfee enterprise products
Use this task to go to the release notes and other product documentation for McAfee enterprise products.

1. Go to knowledge.mcafee.com and select Product Documentation under Useful links.
2. Select <Product Name> | <Product Version> and select the required document from the list of documents.

License attributions

Copyright © 2012 McAfee, Inc. Do not copy without permission.

McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

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