McAfee Policy Auditor 6.0 software

Product Guide for ePolicy Orchestrator 4.6

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Introducing McAfee Policy Auditor

McAfee® Policy Auditor version 6.0 automates the process required for system compliance audits. It measures compliance by comparing the actual configuration of a system to the desired state of a system.

To understand what the software does and how to use it, you must be familiar with these basics:

- What an audit is, when you should use it, and why you should use it.
- The supported deployment solutions based on the type(s) of systems you want to audit.
- The system classifications that determine which functional components can be used.
- The functional components you can use to audit systems. This includes leveraging the software with McAfee Policy Auditor and other McAfee and third-party software.
- The functional components you can use to audit systems. This includes leveraging the software with McAfee® Vulnerability Manager and other McAfee and third-party software.

This document introduces these concepts, successively builds your understanding, and provides details about the use of each functional component. In addition, it helps you understand how the software fits into the framework provided by McAfee® ePolicy Orchestrator®.

Contents

Audience

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

The information in this guide is intended primarily for two audiences:

- Network administrators who are responsible for implementing and enforcing the policy for protecting the company's intellectual property.
- Security officers who are responsible for determining sensitive and confidential data, and defining the corporate policy that protects the company's intellectual property.

Conventions

This guide uses the following typographical conventions.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.

User input or Path	Commands and other text that the user types; the path of a folder or program.
Code	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.
Note	Additional information, like an alternate method of accessing an option.
Tip	Suggestions and recommendations.
Important/Caution	Valuable advice to protect your computer system, software installation, network, business, or data.
Warning	Critical advice to prevent bodily harm when using a hardware product.

Finding product documentation

McAfee provides the information you need during each phase of product implementation, from installing to using and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User Documentation	1 Click **Product Documentation**. 2 Select a **Product**, then select a **Version**. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

Getting started with McAfee Policy Auditor

McAfee Policy Auditor is an extension to ePolicy Orchestrator software software versions 4.5 and 4.6 that automates the process for risk and compliance system audits. Audits can perform tasks such as check system settings, including password length, open or closed ports, file changes, and the presence of software updates.

Contents

Introduction to compliance audits

Before using McAfee Policy Auditor, it is important to understand what audits are, when you should use them, and why you should use them.

What are compliance audits?

A compliance audit is a comprehensive review of an organization's adherence to external regulatory guidelines or internal best practices. McAfee Policy Auditor automates the compliance audit process and allows you to demonstrate compliance to auditors by producing an audit trail showing compliance, compliance history, and actions taken to mitigate risks. Organizations that are out of compliance might be subject to fines or other sanctions, including criminal liability.

When should you use audits?

Use compliance audits when you are subject to government regulations that require your organization to determine system compliance and maintain records. You should also use audits to determine compliance with organizational requirements such as password complexity, password length, the presence of unsupported software, and software patch requirements.

Why should you use audits?

McAfee Policy Auditor automates the process for mandated and organizational audits. Its companion product, McAfee Benchmark Editor, contains built-in benchmarks that the software can use for mandated audits, such as Sarbanes-Oxley (SOX) and the Payment Card Industry Data Security Standards (PCI DSS). The reporting system allows you to demonstrate compliance to auditors while the Findings feature helps you to find solutions to audit issues.

Auditing systems

An audit is an independent evaluation of a computer system to determine whether it is in compliance with corporate and industry security standards. Audit results show recommended improvements to reduce risks.

McAfee Policy Auditor evaluates systems against independent standards developed by government and private industry. It can also evaluate systems against standards that you create yourself. McAfee Policy Auditor uses audits to determine the compliance status of systems and returns results indicating any areas where the system is out of compliance.

Scoring audits

When you audit a system with McAfee Policy Auditor, it returns a score indicating how well the system complied with the audit. McAfee Policy Auditor supports the four scoring models described in the eXtensible Configuration Checklist Description Format (XCCDF) 1.1.4 specifications.

What's new

McAfee Policy Auditor has a number of new features to enhance user experience and expand capabilities.

These are the major new features for this software release:

- **McAfee® Policy Auditor Content Creator** — Allows users to create simple benchmarks and fill in the rule values manually or import them from an existing system.
- **McAfee Benchmark Editor enhancements** — McAfee added these new capabilities to the software:
  - Ability to drag and drop groups
  - Ability to drag and drop rules between groups
  - Ability to delete groups
- **Enhanced display of expired results** — Provides detailed information about expired results to help users determine what steps to take.
- **Server performance improvements** — The server database has been rewritten to speed processing and to eliminate duplicate storage. McAfee added four new dashboards to help users understand the status of audits.
- **Database health tools** — McAfee added daily and weekly server tasks to speed database access by reducing fragmentation and rebuilding fragmented indexes.
- **Improved audit failure status** — McAfee Policy Auditor agent plug-in audit exceptions are logged in the ePolicy Orchestrator software server event log. The exceptions can be seen through a new McAfee Policy Auditor server query and dashboard.
- **Agent debug support** — The McAfee Policy Auditor agent plug-in includes a tool to help you solve problems on managed systems. The tool has these features:
  - **Interface** — Graphical for Windows systems, console for all supported operating systems.
  - **Audits** — Displays and allows you to run available audits.
  - **Benchmarks** — Displays and allows you to run available benchmarks.
  - **Checks** — Displays and allows you to run available checks.
  - **Debug information** — Collect and save information, including the log file and database, to a ZIP file.

- **Entitlement reporting** — Entitlement reporting is an enhancement to the Policy Auditor File Integrity Monitoring feature that produces custom file entitlement reports. It has these capabilities:
    - Monitors file entitlements, such as read and write attributes.
    - Monitors files for changes.
    - Monitors and displays changes to text files.
- **Support for OVAL 5.7 – 5.9** — The software adds support for Open Vulnerability and Assessment Language (OVAL) versions 5.7, 5.8, and 5.9.
- **Support for SCAP 1.1** — The software adds support for Security Content Automation Protocol (SCAP) version 1.1.
- **Agent support for new operating system platforms** — The McAfee Policy Auditor agent plug-in supports these new platforms:
    - HP-UX 11i v2 Itanium
    - HP-UX 11i v3 Itanium
    - Red Hat Enterprise Linux 6.0
    - SuSE Linux Enterprise Server 11

Software components and what they do

McAfee Policy Auditor installs components that help you analyze systems for compliance with recognized, open-source standards and standards that you can create yourself.

These are the McAfee Policy Auditor components as they appear in the interface:

- **Benchmark Editor** — A utility used to enable, disable, create, and edit benchmarks. Each audit must contain at least one benchmark. Ideally, audits should contain only one benchmark.
- **Benchmark Editor Content Distributor** — Distributes content downloaded from McAfee Labs™ to systems.
- **Findings** — Manages findings, which help you understand why an audit check failed and provides information about how to fix the problem.
- **PACore** — The primary portion of the software that controls all other features.
- **PARollup** — Uses the rollup capabilities of ePolicy Orchestrator software to collect summary information from registered ePolicy Orchestrator servers and show aggregated data.
- **Policy Auditor** — Handles policy and task management, audit schedules, and system management.

McAfee Policy Auditor agent plug-in

The McAfee Policy Auditor agent plug-in expands the ability of the McAfee Agent to support McAfee Policy Auditor.

When audits are deployed to systems with the McAfee Agent, the agent plug-in determines when the audits should be run. The agent plug-in conducts audits at the appropriate time and returns the results to the ePolicy Orchestrator server. The agent plug-in can conduct audits when the managed system is off the network, and returns results to the ePolicy Orchestrator server once the system is reconnected to the network.

Installing the agent plug-in adds a product icon to the McAfee Agent system tray. In Windows environments, the product icon optionally displays a balloon tip to indicate the system is being audited.

Systems that have the McAfee Policy Auditor agent plug-in installed are known, in McAfee Policy Auditor terminology, as managed systems.

Use of ePolicy Orchestrator software features

McAfee Policy Auditor is an extension of ePolicy Orchestrator software, and uses and relies upon many of its features.

McAfee Policy Auditor is configured from the ePolicy Orchestrator server. The ePolicy Orchestrator server is the center of your managed environment and provides a single location where you can administer and monitor security settings throughout your network. You can use the default settings or configure the settings to match your organizational needs.

This table lists the applicable ePolicy Orchestrator software features and describes how they are used by McAfee Policy Auditor. You should become familiar with each of the listed features and their uses.

ePolicy Orchestrator feature	Location	Used by McAfee Policy Auditor
Assign Policies	**Menu | Systems | System Tree | Assigned Policies**	To assign policies, like file integrity monitor, to managed systems.
Client tasks	**Menu | Systems | System Tree | Client Tasks**	• To deploy the McAfee Policy Auditor agent plug-in to detected systems. • To update the McAfee Policy Auditor agent plug-into the latest version. • To wake up the McAfee Agent on selected systems.
Contacts	**Menu | User Management | Contacts**	To create user contact information when you want to notify specific personnel by email of an event.
Dashboards and Monitors	**Menu | Reporting | Dashboards**	• To create a new dashboard containing McAfee Policy Auditor monitors • To manage the various dashboards you use for policy audits • To access detailed information about policy audits
Detected Systems (Rogue System Detection)	**Menu | Systems | Detected Systems**	• To identify systems detected by McAfee Foundstone • To determine whether the coverage of network enforcement appliances is sufficient.
Issues	**Menu | Automation | Issues**	To prioritize, assign, and track issues. Issues can also be associated with tickets in a third-party ticketing server.

ePolicy Orchestrator feature	Location	Used by McAfee Policy Auditor
Policy Catalog	**Menu | Policy | Policy Catalog**	• To manage the times when audits are allowed to audit systems. • To manage settings for the file integrity monitor.
Queries	**Menu | Reporting | Queries**	To create and maintain database queries regarding system security information.
Registered Executables	**Menu | Configuration | Registered Executables**	To register a command that can be run on the server as part of an automatic response.
Repositories	**Menu | Software | Master Repository**	To check in and manage content required by McAfee Policy Auditor, such as the Audit Engine content containing all the compliance and threat checks and published benchmarks.
Server Settings	**Menu | Configuration | Server Settings**	To specify parameter values affecting the operations of McAfee Policy Auditor.
Server Tasks	**Menu | Automation | Server Tasks**	• To synchronize data with McAfee Vulnerability Manager using the Maintain McAfee Vulnerability Manager Audits task. • To import McAfee Vulnerability Manager data into McAfee Policy Auditor. • To manage Exemption Expiration. • To process audit results.
Tag Catalog	**Menu | Systems | Tag Catalog**	To create tags that can be used to help organize your systems.
Users	**Menu | User Management | Users**	To create or edit a specific person as a user of McAfee Policy Auditor and their permission type.

Managed systems vs. unmanaged systems

Knowing how McAfee Policy Auditor classifies systems on your network is important for setting up and using the product, and for using its features. McAfee Policy Auditor uses two system classifications: Managed systems and unmanaged systems.

- Managed systems — Systems in the System Tree that have both the McAfee Agent and the McAfee Policy Auditor Agent plug-in installed.
- Unmanaged systems — Systems in the System Tree that do not have the McAfee Policy Auditor agent plug-in installed.

These classifications, and their characteristics and requirements, apply exclusively to McAfee Policy Auditor functionality. Other McAfee products might use the same classifications, but with different characteristics or requirements.

Auditing managed systems

When connected to a network managed by ePolicy Orchestrator software, managed systems can exchange information with the ePolicy Orchestrator server as scheduled. The primary advantage of managed systems is that they are audited by the agent even when they are not connected to the network. When they are reconnected, the Agent plug-in communicates the results to McAfee Policy Auditor. The Agent plug-in slightly increases memory and processor use.

Auditing unmanaged systems

Unmanaged systems can be audited by registering a McAfee Vulnerability Manager 6.8 or McAfee Vulnerability Manager 7.0 server with McAfee Policy Auditor. McAfee Vulnerability Manager performs the audits and returns the results to McAfee Policy Auditor. The primary advantage of unmanaged systems is that you can audit them without installing an agent. Unmanaged systems cannot be audited when they are disconnected from the network.

Configuring McAfee Policy Auditor

McAfee Policy Auditor is configured from the ePolicy Orchestrator server. The server is the center of your security environment, providing a single location from which to administer system security throughout your network.

Contents

Server settings and what they control

McAfee supplies default settings for McAfee Policy Auditor and findings. You can change server settings to fit your organizational needs.

These are the server settings for McAfee Policy Auditor.

Server setting	Description
Audit data retention	As the amount of audit data grows, you can purge all audit data older than a designated date. You can also manage the purge settings for individual audits. In large and complex organizations, the retention times for audit data may vary by audit. The ability to specify data maintenance per audit lowers the cost of maintaining audit data. • **Enable findings data purging** — Allow McAfee Policy Auditor to purge audit results data older than a specified date. This setting is enabled by default. • **Purge findings data after** — Edit to specify how long findings data should be retained. The default setting is 12 months. • **Stop Data Maintenance after** — If the PA: Purge Audit Results server task runs longer than the time specified in this setting, it stops to allow other system data maintenance tasks to run. When the server task restarts, it resumes where it left off. The default setting is to let this task run for 2 hours. • **Remove related Findings results when purging Audit Results** — Select to purge Findings data when purging audit results. This setting is selected by default.
Audit label	Audit labels allow you to use different descriptions for the default labels of Pass, Fail, Pass-Expired, Fail-Expired, or Other-Expired. For example, instead of the word Pass, you can choose to use the word Successful. McAfee recommends that you keep the default settings, because most users find them appropriate and intuitive.

Server setting	Description
Audit score	An audit score indicates how well a system conforms to the ideal settings specified in an audit. McAfee Policy Auditor allows you to change the scoring definitions to reflect your organization's determination of what constitutes a passed or failed audit. • **Minimum High Score** — Any score equal to or greater than this setting means that the system passed the audit. The default setting is 80, meaning that an audit score above 80 is assigned a score category of Pass. • **Audit Score – Fail** — Any audit score equal to or lower than this setting means that the system failed the audit. The default setting is 60, meaning that an audit score below 60 is assigned a score category of Fail. • **Maximum Low Score** — Any score less than the Minimum High Score but higher than the Audit Score - Fail setting means that the audit had mixed results: it neither passed or failed. By default, an audit score between 60 and 80 is assigned a score category of Other.
Audit score categories	McAfee Policy Auditor software provides four categories with default names and colors that describe the success of an audit. You can change the names to fit your organization's requirements, but most users find the default names appropriate and easy to understand. • **High** — The system passed the audit. • **Low** — The system failed the audit. • **Medium** — The system has mixed audit results. Critical systems warrant attention to fix the audit failures, while non-critical systems may be left as is. • **Unknown** — McAfee Policy Auditor is unable to determine whether the system passed an audit. Situations yielding a status of Unknown include systems taken off the network or turned off.
Database Maintenance - allow online rebuild of indexes	Enables database maintenance features, including the rebuilding of indexes.
Database Maintenance - maintain indexes whose fragmentation exceeds this percentage	Specifies the amount of fragmentation that triggers index rebuilding and related maintenance.
Database Maintenance – stop processing after this time	Specifies the amount of time, in hours, that database maintenance tasks run before stopping.
Default Scoring Model	McAfee Policy Auditor supports the four standard eXtensible Configuration Checklist Description Format (XCCDF) scoring models. These scoring models are described in detail in Scoring Audits.
Differentiate expired results in a query	Controls whether expired results are differentiated in a query. You can show expired results as expired or differentiate them as follows: • **pass-expired** — The results have expired but the last audit results evaluated to *pass*. • **fail-expired** — The results have expired but the last audit results evaluated to *fail*. • **other-expired** — The results have expired and the previous audit results evaluated to a condition other than *pass* or *fail*.
Findings data retention	Findings provide information about why checks failed in an audit. This setting defines how long findings information is retained. • **Enable findings data purging** — Allow McAfee Policy Auditor to purge findings information after older than a specified date. By default, this setting is enabled. • **Purge findings data after** — Specifies how long findings data should be retained. The default setting is 12 months. • **Stop Data Maintenance after**— If the FND: Purge Findings server task runs longer than the time specified in this setting, it stops to allow other

Server setting	Description
	system data maintenance tasks to run. When the server task restarts, it resumes where it left off. The default setting is to let this task run for 2 hours.
Frequency to run update audit assignments	Defines the value, in hours, for running the PA: Update Audit Assignments server task. McAfee Policy Auditor sends audit content only to systems that are scheduled to receive the content. This reduces bandwidth and lessens client system disk space requirements.
Full OVAL Results	Allows you to retain full OVAL results for failed, non-patch checks that do not have Findings information. When you enable this setting, the software retains full OVAL results so that you can determine the cause of the failure. This setting is disabled by default and retains "thin" OVAL results, not the full OVAL results.
Max number of FIM version files	Defines the number of file integrity file versions to store. You can store the contents of up to 6 text files, including the baseline version. See the File Integrity Monitoring section for more information on baselines and file versions.
Minimum pass percentage for rule aggregation	When the percentage of rules that pass in an audit exceed the defined percentage, the software will aggregate the results in queries and reports.
Number of benchmark results to purge per batch	The number of benchmark results purged when purging audit results.
Threads for audit results processing	The number of processing threads allotted to audit results. The default number is 5.
Violation limit	Findings provide information about why checks failed in an audit. Since an audit may report thousands of violations, you can limit the number of violation shown in reports through the Violation Limit setting. By default, McAfee Policy Auditor truncates the number of violation results to 300.

Edit McAfee Policy Auditor server settings

Edit the McAfee Policy Auditor server settings to fit your organizational and business needs.

Before you begin

You must be a global administrator to perform this task.

Task

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

1. From the interface, click **Menu | Configuration | Server Settings**.
2. Under Setting Categories, select Policy Auditor. The McAfee Policy Auditor server settings appear in the main panel.
3. Click **Edit**. The settings page appears.
4. Change the settings to the desired values, then click **Save**.

How permission sets work

When McAfee Policy Auditor is installed, it adds a permission group to each permission set. When you create a new permission set, the McAfee Policy Auditor permission group is added to the set. One or more permission sets can be assigned to users who are not global administrators (global administrators have all permissions to all products and features).

Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks. Consider this as you plan your strategy for granting permissions to the users in your environment.

How users, groups, and permission sets fit together

Access to items within ePolicy Orchestrator is controlled by interactions between users, groups, and permission sets. For more information on how they interact, see How users, groups, and permission sets fit together in the McAfee ePolicy Orchestrator 4.6 Software Product Guide.

Default permission sets

McAfee Policy Auditor includes seven default permission sets that provide permissions for McAfee Policy Auditor and related applications.

Permission set	Permissions
PA Admin	**Benchmark Editor** • Activate benchmarks • Edit benchmark tailoring • Create, delete, and apply labels • Create, delete, modify, import, and unlock benchmarks • Create, delete, and import checks **Findings** • View and hide/unhide findings **Issue Management** • Create, edit, view, and purge assigned issues **Policy Assignment Rule** • View and edit rules **McAfee Policy Auditor** • Accept and delete events, and reset system baseline • Allow access to Foundstone Enterprise Manager (EM) • Grant and modify waivers • Allow access to File Entitlement • Add, remove, and change audits and assignments **Policy Auditor Agent** • View and change settings **Policy Auditor Rollup** • View Policy Auditor rollup reports
PA Agent Admin	**McAfee Policy Auditor Agent** • View and change settings

Permission set	Permissions
PA Audit Admin	**Benchmark Editor** • View and export checks • View and export benchmarks **Findings** • View and hide/unhide findings **Issue Management** • Basic: Create issues and edit, view, and purge issues created by or assigned to me **McAfee Policy Auditor** • View Waivers • Allow access to Foundstone Enterprise Manager (EM) • Add, remove, and change audits and assignments
PA Benchmark Activator	**McAfee Benchmark Editor** • Activate benchmarks • View and export checks • View and export benchmarks
PA Benchmark Editor	**McAfee Benchmark Editor** • Edit benchmark tailoring • Create, delete, and apply labels • Create, delete, and import checks • Create, delete, modify, and import benchmarks
PA Viewer	**McAfee Benchmark Editor** • View and export checks • View and export benchmarks **Findings** • View findings **McAfee Policy Auditor** • View waivers • View audits and assignments
PA Waiver Granter	**McAfee Benchmark Editor** • View and export benchmarks • View and export checks **Findings** • View findings **Issue Management** • Create, edit, view, and purge assigned issues **McAfee Policy Auditor** • View audits and assignments • Grant and modify waivers

Edit permission sets

You can edit the default McAfee Policy Auditor permission sets or create your own.

Before you begin

You must be a global administrator to perform this task.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | User Management | Permission Sets**, then select the permission set.
2. Click **Edit** next to the McAfee Policy Auditor permission group. The Edit Permission Set page appears.
3. Select the appropriate options, then click **Save**.
4. Repeat for all appropriate sections of other permission sets.

Using the McAfee Policy Auditor agent plug-in

The McAfee Policy Auditor agent plug-in (agent plug-in) extends the features of the McAfee Agent. It manages the schedule for performing audits, runs the audits, and returns the results to the server.

You install the McAfee Agent and the agent plug-in on managed systems. This enables audits to be conducted even if a system is not connected to the network. Once the system reconnects to the network, it returns audit information to the server and receives updated content and schedules for future audits from the McAfee Policy Auditor server.

Contents

The agent plug-in and how it works

The McAfee Policy Auditor agent plug-in updates the audit schedule on managed systems, launches audit scans according to a schedule, and returns results to the server.

The schedule relies on whiteout and blackout periods that you set. Audit whiteout periods are times when an audit can run on a system or group of systems. Audit blackout periods are times when an audit can't run. The agent plug-in determines the age of the current information and uses any pending blackout or whiteout windows to determine when content should be re-evaluated.

Upon receipt or completion of an audit, the agent plug-in calculates and stores the date and time of the next scheduled audit. You can use the Run Audits feature of ePolicy Orchestrator to force an immediate scan. When you do this, the agent plug-in marks the frequency information as expired and recalculates the date and time for the next scheduled audit. The recalculated date and time are always scheduled during a whiteout period.

The agent plug-in can perform audits when a system is not connected to its network. Once the system reconnects to the network, the agent plug-in returns the results to the server.

Supported platforms

The McAfee Policy Auditor agent plug-in supports a number of Windows, Linux, and Unix-based operating systems.

Operating system	X86 support	X64 support	Other processors	Notes
AIX 5.3 TL8 SP5			Power5, Power6	
AIX 6.1 TL2 SP0			Power5, Power6	
Apple Mac OS X 10.4	X	X	PowerPC	Universal binary
Apple Mac OS X 10.5	X	X	PowerPC	Universal binary
Apple Mac OS X 10.6	X	X	PowerPC	Universal binary
HP-UX 11i v1			RISC	
HP-UX 11i v2			RISC	
HP-UX 11i v2 Itanium			RISC	
HP-UX 11i v3			RISC	
HP-UX 11i v3 Itanium			RISC	
Red Hat Linux AS, ES, WS 4.0	X	X		32-bit agent on 64-bit hardware
Red Hat Enterprise Linux 5.0, 5.1	X	X		32-bit agent on 64-bit hardware
Red Hat Enterprise Linux 6.0	X	X		32-bit agent on 64-bit hardware
Solaris 8			SPARC	
Solaris 9			SPARC	
Solaris 10			SPARC	
SuSE Linux 9	X	X		32-bit agent on 64-bit hardware
SuSE Linux Enterprise Server 10	X	X		32-bit agent on 64-bit hardware
SuSE Linux Enterprise Server 11	X	X		32-bit agent on 64-bit hardware
Windows 2000 Professional	X			
Windows 2000 Server	X			
Windows 2000 Advanced Server	X			
Windows XP Professional	X	X		Native 32- and 64-bit agent
Windows Server 2003 Standard Edition	X	X		Native 32- and 64-bit agent
Windows Server 2003 Enterprise Edition	X	X		Native 32- and 64-bit agent
Windows Vista	X	X		Native 32- and 64-bit agent
Windows 2008 Server	X	X		Native 32- and 64-bit agent
Windows 7	X	X		Native 32- and 64-bit agent

How content is managed

Content for McAfee Policy Auditor consists of benchmarks and checks. The content package is included when the product is installed, and is placed into the ePolicy Orchestrator master repository.

Before you can use benchmarks in audits, you must activate them in McAfee Benchmark Editor. See the McAfee Benchmark Editor Product Guide for information about how to do this.

The master repository is updated daily by a server task that is included with the software. If you want to update McAfee Policy Auditor on a different schedule, you can create a new server task. You must verify that the task is enabled.

The master repository is configured when installed. However, you must ensure that proxy server settings, if any, are configured correctly. By default, ePolicy Orchestrator uses Microsoft Internet Explorer proxy settings.

For information about repository management, proxy settings, and server tasks, see the ePolicy Orchestrator software documentation.

Install and uninstall the agent plug-in

Managed systems under McAfee Policy Auditor must have the McAfee Agent and the McAfee Policy Auditor agent plug-in.

For information on installing and working with the McAfee Agent, see the ePolicy Orchestrator documentation.

Tasks

▶ Install the McAfee Policy Auditor agent plug-in
▶ Uninstall the agent plug-in
▶ Send a manual wake-up call to a group of systems

Install the McAfee Policy Auditor agent plug-in

Install the McAfee Policy Auditor agent plug-in before you run audits on managed systems.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Systems | System Tree** then click the **Systems** tab.
2. Select the System Tree group containing the systems on which you want to install the agent plug-in.
3. Click **Actions | New Tasks**. The Description page of the Client Task Builder appears. Fill in the settings, then click **Next**.
   - **a** Type an appropriate name for the task, such as Install McAfee Policy Auditor Windows agent plug-in.
   - **b** Optionally, provide a description in the Notes text box.
   - **c** From the Type drop-down list, select **Product Deployment**.

   d. In Tags, select which systems in the selected group on which you want to install the agent plug-in.
      - **Send this task to all computers** — Install the agent plug-in on all systems in the selected group.
      - **Send this task to only computers which have the following criteria** — Use the edit buttons to include or exclude systems with tags. See the ePolicy Orchestrator documentation for information on working with tags.

4. Fill in all settings on the Configuration page, then click **Next**.
   a. Select **Windows** for the Target Platform.
   b. For Products and components, select these options from the drop-down lists.
      - **McAfee Policy Auditor for Windows 6.0.0**.
      - **Action** — Install.
      - **Language** — The language used on the systems.
      - **Branch** — Current.

   c. For Options, you can select **Run at every policy enforcement (Windows only)** to re-install the plug-in at the next policy enforcement interval if a user has removed the product or component.
   d. Click **Next**. The Schedule page appears.
5. Configure the schedule details as needed, then click **Next**.
6. Review the task settings, then click **Save**. The task is added to the list of client tasks for the selected group and any group that inherits the task.
7. To run the client task immediately, send a manual wake-up call to the systems.

Uninstall the agent plug-in

Uninstall the McAfee Policy Auditor agent plug-in from systems on your network if you do not want them to be managed by McAfee Policy Auditor content. This is useful when you want to convert a managed system to an unmanaged system and reduce the load on system resources.

Task

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

1. Follow the procedure for installing the agent plug-in. On the Configuration page, select **Remove** from the **Action** drop-down list. Set the other options as needed
2. Review the task settings on the Summary page, then click **Save** to store the task.
3. Send a manual wake-up call to run the task immediately.

Send a manual wake-up call to a group of systems

Send manual wake-up calls to a System Tree group to verify that the McAfee Agent and ePolicy Orchestrator server are communicating. This is useful when you make policy changes and want agents to download the update.

Before you begin

Before sending the agent wake-up call to a group, make sure that wake-up support for the systems' groups is enabled and applied on the General tab of the McAfee Agent policy pages. This is enabled by default.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Systems | System Tree**, then select the group in the System Tree.
2. Select the systems from the list, then click **Actions | Wake Up Agents**. The Wake Up McAfee Agent page appears.
3. Verify that the systems appear next to **Target systems**.
4. Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or a **SuperAgent Wake-Up Call**.
5. Accept the default **Randomization** (0 – 60 minutes) or type a different value.

   NOTE: If you type 0, agents respond immediately. Consider carefully the number of systems that are receiving the wake-up call and how much bandwidth is available.

6. By default, **Get full product properties** is selected. This causes the agent plug-in to send complete system properties to McAfee Policy Auditor. Deselect this option if you want to send only properties that have changed since the last agent-server communication.
7. Click **OK** to send the wake-up call.
8. Verify that the agent plug-in and ePolicy Orchestrator server are communicating: go to **Reporting | Audit Log** and search the log for an entry Wake Up Agents | Succeeded.

Display the system tray icon on Windows systems

You can configure McAfee Policy Auditor to display a system tray icon on Windows systems. The icon cannot is not available for non-Windows systems.

The icon allows the user to see the status of audits, including whether an audit is running, scheduled, not scheduled, or disabled. It optionally displays a balloon tip to indicate that the system is being audited.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Systems | System Tree**, then click the **Assigned Policies** tab.
2. From the **Product** drop-down list, select **Policy Auditor Agent**.
3. Under the **Policy** column in the My Default row, click **Edit Settings**. The whiteout/blackout page appears.
4. Next to General Options, select **Show the Policy Auditor system tray icon (Windows only)**, then click **Save**.

Configuring agentless audits

McAfee Policy Auditor can register a McAfee Vulnerability Manager 6.8 or 7.0 (formerly Foundstone) server to conduct agentless audits.

Agentless audits allow you to audit systems that do not have the McAfee Policy Auditor agent plug-in installed. McAfee Vulnerability Manager searches for systems using a Host Name or IP range, adds them to the System Tree, and conducts agentless audits.

Installing the Foundstone ePO Data Integration (ePO 4.5 server or ePO 4.6 server) allows you to import McAfee Vulnerability Manager data into your ePolicy Orchestrator database and view that data in reports.

To use the extension with ePolicy Orchestrator software, you must also have an existing McAfee Vulnerability Manager installation with scanned asset data.

Contents

How McAfee Policy Auditor integrates with the McAfee Vulnerability Manager extension

McAfee Policy Auditor and McAfee Vulnerability Manager integrate seamlessly to gather data, share information, and perform both agent- and system-based audits.

Systems with the agent plug-in installed are referred to as managed systems. Systems without the agent plug-in are called unmanaged systems.

Uniform system management

McAfee Policy Auditor and McAfee Vulnerability Manager support uniform system management under ePolicy Orchestrator software.

Managed and unmanaged system are supported the same way:

- Assets from a McAfee Vulnerability Manager Discovery Scan are matched to system already managed by the ePolicy Orchestrator server to avoid duplication. Each system is uniquely identified. Systems with duplicate names can be added to the System Tree, but they are still managed as different systems.
- A System Tree group can contain both managed and unmanaged systems.

- When you change a system from unmanaged to managed, this distinction is reflected in queries and page views.
- McAfee Policy Auditor supports an all agent-based System Tree, an all agentless System Tree, and a mix of agent-based and agentless devices. A group can contain both managed and unmanaged systems.
- Communication between McAfee Policy Auditor and McAfee Vulnerability Manager is through a single channel and can pass through common firewall configurations without reconfiguration.

McAfee Vulnerability Manager extension integration with scannable systems

The McAfee Vulnerability Manager extension can scan most operating systems supported by McAfee Policy Auditor.

McAfee Vulnerability Manager can scan these operating systems:

Windows 2000 Server
Windows 2000 Advanced Server
Windows 2000 Professional
Windows XP Professional
Windows Server 2003 Standard Edition
Windows Server 2003 Advanced Edition
AIX 5.3, 6.1
Windows Server 2003 Enterprise Edition
Windows 2008 Server
Solaris 8
Solaris 9
Solaris 10
Red Hat Enterprise Linux 5.0, 5.1

Asset Discovery scans

ePolicy Orchestrator software supports the manual and automatic importing of systems into the System Tree.

When McAfee Vulnerability Manager discovers new systems during a McAfee Vulnerability Manager Asset Discovery Scan, it designates them as rogue systems. Regardless of how assets are imported, users must add, or promote, them to the ePolicy Orchestrator server System Tree before they can be audited.

McAfee Vulnerability Manager can only audit systems that have a Foundstone ID. The association between a system and a Foundstone ID is established when a system is imported from McAfee Vulnerability Manager and added to the System Tree.

Data collection scans

The McAfee Vulnerability Manager extension uses the Data Collection Scan to audit systems and gather compliance data. For audit results to remain current, the scan must be scheduled with sufficient time to audit systems before running the the PA: Maintain Foundstone server task.

The Maintain Foundstone Audits server task

The Maintain Foundstone Audits server task is responsible for setting audit frequency requirements, synchronizing audit information, distributing audit content, and performing cleanup tasks.

The installation application automatically creates a server task named PA: Maintain Foundstone audits when you install the McAfee Vulnerability Manager extension. The task runs once per day by default. If you need to change the schedule, you should schedule it to run after the Data Collection Scan has had the opportunity to conduct audits so that audit results stay current.

The purpose of the PA: Maintain Foundstone audits server task is to:

- Adhere to audit frequency requirements by requesting audit results from McAfee Vulnerability Manager for any systems whose results expire within the next 24 hours. The task does not retrieve results from McAfee Vulnerability Manager, but requests McAfee Vulnerability Manager to update and assemble audit results from data in preparation for scanning systems and returning the results to McAfee Policy Auditor.
- Synchronize information between McAfee Vulnerability Manager and McAfee Policy Auditor. For example, if you add or delete an audit from McAfee Vulnerability Manager, the task will add or delete an audit from McAfee Policy Auditor.
- Distribute content, such as benchmarks, to the McAfee Vulnerability Manager server. If the benchmark has been updated on the ePolicy Orchestrator server, the task will update the benchmark on the McAfee Vulnerability Manager server.
- Perform assorted cleanup tasks on the McAfee Vulnerability Manager server.

The Data Import server task

McAfee Vulnerability Manager uses the MVM Data Import server task to populate the ePolicy Orchestrator server database with system data from the McAfee Vulnerability Manager database.

The server task automatically gathers new McAfee Vulnerability Manager database asset data on a regular schedule. For audit results to remain current, the task must be scheduled to run after the PA: Maintain Audits Server task has finished running.

Server support

Before configuring McAfee Vulnerability Manager server, it is important to understand how McAfee Vulnerability Manager and ePolicy Orchestrator work together.

One McAfee Vulnerability Manager server can support multiple ePolicy Orchestrator servers running McAfee Policy Auditor. However, an ePolicy Orchestrator server running McAfee Policy Auditor can only integrate with one McAfee Vulnerability Manager server.

Configure McAfee Vulnerability Manager and the ePolicy Orchestrator extension

You can configure McAfee Vulnerability Manager and the McAfee Vulnerability Manager extension to discover systems, collect data, and synchronize this information with McAfee Policy Auditor.

Tasks

- ▶ Create a McAfee Vulnerability Manager workgroup
- ▶ Configure the McAfee Vulnerability Manager single sign-on feature
- ▶ Create a data source to synchronize McAfee Vulnerability Manager and ePolicy Orchestrator
- ▶ Register a McAfee Vulnerability Manager database server with McAfee Policy Auditor

- Manage McAfee Vulnerability Manager credential sets
- Create an Asset Discovery scan
- Create an MVM Data Import task
- Add systems found by McAfee Vulnerability Manager scans to the System Tree
- Create a Data Collection Scan
- View McAfee Vulnerability Manager scan status

Create a McAfee Vulnerability Manager workgroup

Create a McAfee Vulnerability Manager workgroup and administrator for your McAfee Policy Auditor administrator and users.

McAfee recommends that you give the McAfee Policy Auditor administrator only the access of a McAfee Vulnerability Manager workgroup administrator, not full access of an organization administrator. Workgroup administrators can make changes that affect their workgroup only. Organization administrators can make changes that affect the whole organization, including workgroups unrelated to the McAfee Policy Auditor group.

You must perform this task in the McAfee Vulnerability Manager Enterprise Manager.

Before you begin

Before you can create a McAfee Vulnerability Manager workgroup, you must:

- Install and set up McAfee Vulnerability Manager.
- Create an organization.
- Specify an administrator for the organization.

Task

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

1. From McAfee Vulnerability Manager Enterprise Manager, go to **Manage | Users/Groups**.
2. Select the organization that you have already created.
3. Right-click the organization and select **New Workgroup**.
4. On the General page, type the workgroup name and description, then click **Next**. The IP Pool page appears.
5. Type the IP ranges to be used in this workgroup, then click **Next**. The Administrator page appears.
6. Type the information for the workgroup administrator.
7. Click **Finish**.

Configure the McAfee Vulnerability Manager single sign-on feature

You can enable the McAfee Vulnerability Manager single-sign-on feature in McAfee Policy Auditor. This gives McAfee Policy Auditor users access to portions of the McAfee Vulnerability Manager Enterprise Manager.

Before you begin

Using single sign-on requires that you create a McAfee Vulnerability Manager workgroup.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Configuration | Server Settings** and select Foundstone API Server.
2. Click **Edit**, select **Enable Policy Auditor to use these server settings**, and type an organization, user name, and password.
3. Click **Save**.
4. Go to **Automation | Server Tasks**.
5. Click **Run** for the PA: Maintain Foundstone audits server task. The Server Task Log page appears and the Status column shows that the task is In Progress. The task might take several minutes or more to run. If the final status of the task is Completed, Single Sign-On is properly configured.
6. Verify that Single Sign-On is properly configured by going to **Systems | Audits** and confirming that these links appear on the page:
   - Edit Foundstone Scans
   - View Foundstone Scan Status
   - Manage Foundstone Credential Sets
   - Manage Foundstone Data Sources

Create a data source to synchronize McAfee Vulnerability Manager and ePolicy Orchestrator

You must synchronize McAfee Vulnerability Manager data with ePolicy Orchestrator server data. This avoids duplication by ensuring that systems and other assets from a McAfee Vulnerability Manager Discovery Scan are matched to ePolicy Orchestrator server-managed assets.

You can also set up a data source from the McAfee Vulnerability Manager interface. See the McAfee Vulnerability Manager documentation for details on how to do this.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Risk & Compliance | Audits | Manage Foundstone Data Sources**. A new McAfee Vulnerability Manager browser window appears.
2. Click **Add Data Source**.
3. Enable McAfee Vulnerability Manager to connect to the ePolicy Orchestrator database server by providing a name, data source type, ePolicy Orchestrator server address, ePolicy Orchestrator server database name, ePolicy Orchestrator database server user name, and password.

   NOTE: If you leave the user name and password blank, the data synchronization service will try to use the account that the data synchronization service is configured to for authentication of the ePolicy Orchestrator database server. This requires configuring the service to run as a domain user that has access to the ePolicy Orchestrator database server.

4. Select **Active** in the Scheduler pane.

5 Select a Schedule Type and set the scheduling options.

6 Determine how you want to configure the McAfee Vulnerability Manager Integration pane. Select ePolicy Orchestrator server to received the data and select the appropriate McAfee Vulnerability Manager organization or workgroup. Click **Save**.

7 Refresh the McAfee Vulnerability Manager browser window, select the scan you created and, if the scan has not been activated, click **Activate**.

Register a McAfee Vulnerability Manager database server with McAfee Policy Auditor

Configure your McAfee Vulnerability Manager Database server as a registered server.

Before you begin

You must have an existing McAfee Vulnerability Manager Database server, with scanned asset data, to use the McAfee Vulnerability Manager extension.

Task

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

1 In the ePolicy Orchestrator user interface, click **Menu | Configuration | Registered Servers**, then click **New Server**.

2 From the **Server type** drop-down list, select **Vulnerability Manager**. Click **Next**.

3 Type the McAfee Vulnerability Manager Database server host name or IP address. For example, type myhost or 123.45.67.89.

4 Select a **Server instance** and type the appropriate information.

   - Select **Default** if Microsoft SQL 2005 was installed with the default settings.
   - Select **Instance name** if the Microsoft SQL 2005 name was changed and type the instance name.
   - Select **Port number** if you are required to specify a port number for the IP address and type the port number.

5 **Required to use SSL to connect** is enabled by default. The ePolicy Orchestrator server requires an SSL connection to communicate with the McAfee Vulnerability Manager Database server.

6 Type the McAfee Vulnerability Manager Database server name in the **Database name** field. The default is Faultline.

7 Select the appropriate **Authentication type**.

   - Select Windows authentication to enter a Windows user name and password to access the McAfee Vulnerability Manager database server. The user name for Windows authentication must include the domain (domain\user).
   - Select SQL authentication to enter a SQL user name and password to access the McAfee Vulnerability Manager Database server.

8 Click **Test Connection** to determine whether the ePolicy Orchestrator server can connect to the McAfee Vulnerability Manager database. If the McAfee Vulnerability Manager Database server is inaccessible (for example, offline), then the test connection will fail. A successful test connection is not required for saving your Registered Server information.

Manage McAfee Vulnerability Manager credential sets

You can create, edit, and delete credential sets for systems managed by McAfee Vulnerability Manager. Credential sets grant McAfee Vulnerability Manager access to systems and, depending on the operating system, may use Windows authentication or a user name with password.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Risk & Compliance | Audits | Manage Foundstone Credential Sets**. The Credential Sets browser window opens.
2. On the Start tab, edit the name and description of the credential set.
3. Select credentials and click the appropriate account type in the System Tree or from the **Account Type** drop-down list. Type the required credential information in the appropriate fields. Click **Add**.
4. You can specify multiple credentials, such as credentials for each domain in the search range, and click **Add** after specifying each credential. Consult the McAfee Vulnerability Manager documentation for details on other settings for this tab.
5. Click **Save**.

Create an Asset Discovery scan

Create a McAfee Vulnerability Manager Asset Discovery scan to find systems in user-specified IP ranges. After you create and runa an asset discovery scan, create an run an MVM Data Import task, then add systems found by the scans to the System Tree.

Consult the McAfee Vulnerability Manager documentation for details on Asset Discovery scan settings.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Risk & Compliance | Audits**, then click **Edit Foundstone Manager Scans**. The Scan Configuration page opens in a new browser window.
2. Click **New Scan**. The Scan Details page opens in a new browser window. Select **Use a Vulnerability Manager template** and click **Next**. The Vulnerability Templates appear.
3. Select **Asset Discovery Scan** and click **Next**.
4. Type a descriptive name for the scan and select **Custom** from the **Type** drop-down list.
5. McAfee Vulnerability Manager offers three methods to search for systems or to exclude systems from scans. Use one or more of these three methods to include or exclude systems.
   - **Targets** tab — Supply any combination of a host name, IP address range, or CIDR Address. Click **View Global Pool** to see the available IP range.
   - **Browse** tab — Drag and drop listed systems into the Included Ranges or Excluded Ranges panes.
   - **Search** tab — Select a search type under **General Filter** and type an appropriate search phrase or IP address in the **String to search for** text box. Alternatively, you can select one or more checkboxes in the **Criticality Filter**. You can also combine **General Filter** and **Criticality Filter** searches. Click the **Search** button to return a list of assets matching your search criteria.

6 Click **Next**. The Settings tab appears.

7 Select credentials and click on the appropriate account type in the tree pane or from the **Account Type** drop-down list. Type the required credential information in the appropriate fields. Click **Add**.

8 You can specify multiple credentials, such as credentials for each domain in the search range, and click **Add** after specifying each credential. Click **Next**. The Reports tab appears.

9 Deselect **Create remediation tickets**. The Scheduler tab appears.

10 Select a Schedule Type. McAfee recommends that you select the **Immediate** option the first time you run this scan. Once McAfee Vulnerability Manager has had the opportunity to scan all assets, you can edit the scan to occur at regular intervals.

11 Click **OK** to save the scan.

Create an MVM Data Import task

Create an MVM Data Import task to populate the ePolicy Orchestrator database with system data from the McAfee Vulnerability Manager database. The task automatically gathers new McAfee Vulnerability Manager database system data on a regular schedule.

Before you begin

You must have a Registered Server set up before you begin this task.

Task

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

1 In the ePolicy Orchestrator user interface, click **Menu | Automation | Server Tasks**, then click **New Task**.

2 Type a **Name** and, optionally, **Notes** for the task. McAfee recommends naming the task Foundstone Data Import.

3 Select **Enabled** and click **Next**.

4 Select **MVM Data Import** from the **Actions** drop-down list.

5 Select a McAfee Vulnerability Manager server from the **Server Name** list.

6 Select one of the **Import Data** types to control how the data is imported.

Use this...	To do this...
Delta	Imports only new data since the last time McAfee Vulnerability Manager data was imported. If there is no McAfee Vulnerability Manager data in the ePolicy Orchestrator database, all available Vulnerability Manager data is imported.
All	Overwrites all McAfee Vulnerability Manager data in yourePolicy Orchestrator database with current McAfee Vulnerability Manager data.

7 Click **Next**. The Scheduling page appears. Select scheduling options for this task, then click **Next**. The summary page appears.

8 Review the summary information before saving this task.

9 Click **Save**.

Add systems found by McAfee Vulnerability Manager scans to the System Tree

You can add systems discovered during a McAfee Vulnerability Manager scan to the ePolicy Orchestrator server System Tree.

To use systems discovered by a McAfee Vulnerability Manager scan in McAfee Vulnerability Manager, the user must import the systems into the ePolicy Orchestrator server and make them available through the System Tree.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Systems | Detected Systems**.
2. Select a **Subnet** in the **Top 25 Subnets** pane.
3. Select systems that you want to add to a System Tree group from the **Rogue System Interfaces by Subnet** list. Click **Add to System Tree**. The Add to System Tree page appears.
4. Click **Browse** and select a System Tree group.
5. Select **Allow duplicate entries to be added to the System Tree** only if you wish to allow duplicate entries in the System Tree.
   Caution: McAfee recommends caution when selecting this box, but there are valid reasons to use this feature. For example, you might have two systems with the same name but different IP addresses.
6. Click **Add** to add the selected systems to the selected group.
7. Repeat steps 2–6 to add other systems to System Tree groups.

Create a Data Collection Scan

Create a McAfee Policy Auditor Data Collection Scan to conduct audits requested by McAfee Policy Auditor.

NOTE: Agentless audits conducted by McAfee Vulnerability Manager do not honor whiteout and blackout periods.

Task

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

1. In the ePolicy Orchestrator user interface, click **Menu | Risk & Compliance | Audits**, then click **Edit Foundstone Scans**. The Scan Configuration page opens in a new browser window.
2. Click **New Scan**. The Scan Details page opens in a new browser window. Select **Use a Vulnerability Manager template** and click **Next**. The Vulnerability Templates appear.
3. Select **McAfee Policy Auditor Data Collection Scan** under the XCCDF Templates section. Click **Next**.
4. Supply a descriptive name for the scan and select **Custom** from the **Type** drop-down list.
5. McAfee Vulnerability Manager offers three methods to search for assets or to exclude systems from scans. Select one method or any combination of the three methods to include or exclude systems. When finished, click **Next**. The Settings tab appears.

6 Select **Credentials** and click on the appropriate account type in the tree pane or from the **Account Type** drop-down list. Type the required credential information in the appropriate fields. Click **Add**.

7 You can specify multiple credentials, such as credentials for each domain in the search range, and click **Add** after specifying each credential. Consult the McAfee Vulnerability Manager documentation for details on other settings for this tab. Click **Next**. The Scheduler tab appears.

8 Select the appropriate schedule type and settings. Click **OK** to save the scan.

TIP: McAfee recommends that you select the **Immediate** option. Once McAfee Vulnerability Manager has had the opportunity to scan for systems, you can change the scan to occur at regular intervals.

View McAfee Vulnerability Manager scan status

You can view the status and results of McAfee Vulnerability Manager scans. The Asset Discovery Scan needs to finish running before you add assets to the ePolicy Orchestrator System Tree.

Task

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

1 In the ePolicy Orchestrator user interface, click **Menu | Risk & Compliance | Audits | View Foundstone Scan Status**. The Scan Status page opens in a new browser window. The **Status** column shows the scans that are complete.

2 Click to view the scan report.

How to handle missing audit results

McAfee Policy Auditor uses the concept of frequency to determine how often audit data should be gathered. Frequency is defined as "Audit results should be no older than *nnn* time unit," where "nnn" is a number and "time unit" is "days," "weeks," and "months." For example, if the frequency for an audit is defined as one month and a managed system has not been audited in more than one month, the system is out of frequency and its status is unknown.

The McAfee Vulnerability Manager extension uses the Data Collection Scan to audit systems and gather compliance data. The Data Collection Scan must finish before the PA: Maintain Foundstone server task is run.

When the PA: Maintain Foundstone server task runs, it requests audit results for any missing results, any expired results, or any results that will expire within the next 24 hours. Thus, audits with a one-day frequency is set for auditing every time the PA: Maintain Foundstone audits server task is run. The task also assembles previously-collected audit results, synchronizes information, and performs cleanup tasks.

The PA: Maintain Foundstone audits server task must be given a sufficient amount of time to assemble data before the MVM Data Import server task is run. The MVM Data Import task collects the latest asset data and imports it into the ePolicy Orchestrator server database. McAfee Policy Auditor then has the latest information to appear in reports and queries.

To make sure that your audit results are up to date, configure the Data Collection Scan, PA: Maintain Foundstone audits server task, and MVM Data Import server task to give the system enough time to conduct audits and assemble result data.

Troubleshoot missing audit results

Configure McAfee Vulnerability Manager to ensure that the latest audit results appear in queries and reports.

The Data Collection Scan, PA: Maintain Foundstone audits server task, and MVM Data Import server task can all be run manually from the interface.

If systems are not being audited because they are disconnected from the network, you can run the scan and server tasks more frequently or convert them to managed systems by installing the McAfee Policy Auditor agent plug-in. A managed system audits itself and returns the results once it is reconnected to the network.

Task

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

1. Schedule the Data Collection Scan to audit systems and gather data. The scan must be given enough time to do its work and the schedule should match the smallest audit frequency. For example, if you schedule quarterly, monthly, and weekly audits, you should schedule the Data Collection Scan to run at the beginning of every week.
2. Schedule the PA: Maintain Foundstone audits server task to run after the Data Collection Scan has had enough time to complete. Click **Menu | Risk & Compliance | Audits | View Foundstone Scans** to determine how long the Data Collection Scan takes to run and schedule the Maintain McAfee Vulnerability Manager server task appropriately.
3. Schedule the MVM Data Import server task to run after the PA: Maintain Foundstone audits server task has had enough time to complete.

How to handle mismatched McAfee Vulnerability Manager certificates

Certificates are sets of electronic files created by a trusted Certificate Authority. They contain encrypted information that allows others to verify their origin. On a network, certificates allow systems to create a trust relationship that allows them to exchange information using encrypted communication.

The McAfee Vulnerability Manager 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 both 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.

Mismatched certificates

There are two situations when your McAfee Policy Auditor does not match the McAfee Vulnerability Manager server certificates.

- **Repairing Policy Auditor** — Clicking **Repair** for McAfee Policy Auditor in Add or Remove Programs does not reinstall new McAfee Vulnerability Manager Configuration Manager certificates. The repair option reconnects with McAfee Vulnerability Manager Configuration Manager, but the certificates are old and SSL communication fails.
- **Connecting to a new or different McAfee Vulnerability Manager server** — Connecting to a new or different McAfee Vulnerability Manager server does not automatically install new certificates.

Troubleshoot mismatched McAfee Vulnerability Manager certificates

Use this task to re-establish or change SSL communication between McAfee Policy Auditor and a McAfee Vulnerability Manager server.

Task

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

1. From the McAfee Vulnerability Manager Configuration Manager, select the McAfee Policy Auditor server that needs new certificates.
2. Click **Tasks**, then select **Install Customer-Specific Certificate**.
3. Click **Initiate Task**. McAfee Vulnerability Manager Configuration Manager distributes the customer-specific certificate to McAfee Policy Auditor. View the System Messages to ensure the task completed successfully.
4. Follow the tasks in *Configuring McAfee Vulnerability Manager and the McAfee Vulnerability Manager extension* to complete the setup.

Creating and managing audits

McAfee Policy Auditor allows you to create audits based on benchmarks and assign them to run on systems.

You can create audits from a McAfee-supplied selection of predefined benchmarks established by government and industry such as SOX, HIPAA, PCI, and FISMA. You can also create audits based on third-party benchmarks or benchmarks that you create yourself.

Audits return results that include a score allowing you to determine how well a system complies with the rules in the benchmark.

Contents

Audits and how they work

McAfee Policy Auditor evaluates systems against independent standards that are developed by government and private industry. It can also evaluate systems against standards that you create.

The software uses audits to determine the compliance status of a system, and returns results indicating areas that are out of compliance.

An audit consists of:

- A benchmark or a selected profile within a benchmark
- A system or groups of systems
- An audit frequency (how often the data should be gathered)
- An optional waiver to temporarily exclude systems or audit results from reports

Benchmarks are documents that contain rules for describing the desired state of a system according to recognized standards. Rules contain one or more checks that are normally written in the OVAL language. See the documentation for McAfee Benchmark Editor to learn more about benchmarks and their structure.

When you run an audit against a system, the audit reports the comparison between the configuration status of the system and the rules in the benchmarks. When the default audit scoring model is used, the audit also reports a comparative score of the system ranging from 0 to 100.

Audit frequency

Audit frequency describes how often data should be gathered.

Frequency is defined as "Audit results should be no older than *nnn* time unit," where "nnn" is a number and "time unit" is days, weeks, or months. For example, if the frequency for an audit is defined as 1 month and a system has not been audited in more than 1 month, the results are considered to have expired.

Differentiating expired results

When you set the Differentiate expired results in a query server setting to true, reports and queries differentiate expired results as follows:

- **pass-expired** — The results have expired but the last audit results evaluated to pass.
- **fail-expired** — The results have expired but the last audit results evaluated to fail.
- **other-expired** — The results have expired and the previous audit results evaluated to a condition other than pass or fail.

No audit results

If an audit has not run, it has a status of no results in reports and queries. Results are shown after the audit runs.

When audits are run

McAfee Policy Auditor provides three ways to run an audit.

The software runs audits under these situations:

- You manually run an audit. When you manually run an audit, the audit runs during the next whiteout period.
- The audit is scheduled to run.
  - Managed systems — The agent plug-in runs the audit before the results expire, even if the system is not connected to the network. The audit expiration date is defined by the audit frequency.
  - Unmanaged systems — McAfee Foundstone or McAfee Vulnerability Manager runs the audit before the audit expires, as defined by the audit frequency. The system must be connected to the network.
- McAfee updates the audit content. This happens most often with patch assessment audits. When content is updated, the audit runs during the next whiteout period.

Per audit data maintenance

McAfee Policy Auditor provides per audit data maintenance. This lets you control, at the individual audit level, what information to retain and how long to retain it.

The software system settings provide a standard for retaining results for audits and Findings. However, you may want to retain some audit information for a greater or lesser amount of time.

You can create or edit an audit so that it retains audit or Findings information for a different period of time than is specified in the global system settings.

Benchmark profiles and their effect on audits

Audits have benchmarks assigned to them. Many benchmarks contain profiles, which are named sets of selected groups, rules, and values targeted toward different computer system configurations and threat risks. A profile can:

- Enable or disable one or more groups
- Enable or disable one or more rules
- Change the variables that are used within a rule, such as the minimum password length

Profiles are normally designed to apply to a particular set of systems. For example, a benchmark could contain two profiles, one for Windows and one for UNIX. As another example, a benchmark might contain *High Security*, *Medium Security*, and *Low Security* profiles.

Selecting a profile should be based upon the risk of the systems being audited. Systems containing customer credit card information are a greater threat to an organization if the data is compromised than does a system used to create company newsletters.

Considerations for including systems in an audit

Audits can be designed for a specific computer system configuration, and McAfee Policy Auditor allows you to include or exclude systems from an audit based on a number of system characteristics.

McAfee Policy Auditor allows you to exclude one or more managed systems based on system name, IP address, MAC address, or user name.

Including systems in an audit

McAfee Policy Auditor provides two methods for including systems in an audit.

The first method allows you to include managed systems by specifying System Tree and Tags:

- **Add System** — A managed system as defined by system name, IP address, MAC address, or user name
- **Add Group** — A group defined in the ePO System Tree
- **Add Tag** — Systems that have been tagged in the ePO System Tree, such as server, workstation, or laptop.

The second method allows you to include managed systems by specifying *Criteria*. Criteria is defined by selecting properties and using comparison operators and values to represent managed systems. You can select one or more criteria.

Benchmark labels and how they are used

Labels classify a benchmark to aid in searches. Each benchmark can have multiple labels assigned to it.

Labels can describe the programmatic use of a benchmark, such as applying a label of MNAC to a benchmark designed for the McAfee Network Access System extension. Labels can also describe the function of a benchmark, such as applying a label of SOX to a benchmark that tests compliance with the Sarbanes-Oxley standard. Labels are applied with the McAfee Benchmark Editor extension or are contained in McAfee-supplied benchmarks.

When you assign a benchmark to an audit, the benchmark selection process provides a drop-down list showing all available benchmark labels. This tool allows you to filter benchmarks based on the label that you want to use for your audit.

Findings

McAfee Policy Auditor provides enhanced results for checks, also known as findings.

Findings results appear in monitors and queries and include additional information about the state of a system that is helpful to security officers and network administrators when fixing issues. Findings are included in reports and provide additional information in audit results. For example, if an audit expects a password with at least 8 characters but finds a password with only 6 characters, the Findings show the actual and expected results.

Since it is possible to create a check that reports thousands of violations. McAfee Policy Auditor allows you to set a violation limit that reduces the number of violations that can be displayed to conserve database resources. Setting the violation limit to 0 causes monitors and queries to display all violations.

Agentless audits

When you create an audit, McAfee Policy Auditor provides the capability to create audits that use McAfee Vulnerability Manager (formerly Foundstone®) for some or all audits. If McAfee Policy Auditor is integrated with Foundstone, this is controlled by the **Use Foundstone to audit all systems** checkbox on the Properties page of the New Audit Builder. This table shows how McAfee Policy Auditor uses Foundstone to audit systems.

Option	Definition
Select **Use Foundstone to audit all systems**	Uses Foundstone to conduct agentless audits of all selected systems.
Deselect **Use Foundstone to audit all systems**	• Uses the McAfee Policy Auditor agent plug-in to conduct audits of systems with the plug-in. • Uses Foundstone to conduct agentless audits of systems that have been imported correctly into the System Tree.

Activate benchmarks

You must activate a benchmark in McAfee Benchmark Editor before you can include it in an audit.

Task

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

1 Click **Menu | Risk & Compliance | Benchmarks**.

2 Find the benchmark to use in your audit and check its status. If the status is not *active*, select it and click **Actions | Activate**.

The benchmark is activated and appears in the list of available benchmarks when you create an audit.

Create an audit

Audits determine whether systems comply with your security needs and the results tell you what, if anything, needs to be done to make the systems compliant.

Before you begin

- You must have permissions to add, remove, and change audits and assignments.
- You must have a benchmark that you have activated for use in the audit.
- McAfee Policy Auditor must be integrated with McAfee Vulnerability Manager if you plan to create an agentless audit.

Task

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

1. Click **Menu | Risk & Compliance | Audits**, then click **Actions | New Audit**. The New Audit Builder appears.
2. Select a platform and label to filter the benchmarks in the Active Benchmarks pane. For example, select the Microsoft Windows platform and the FISMA label to show only Windows benchmarks that have a FISMA label.
3. In the Active Benchmarks pane, select one or more benchmarks and click **Add Benchmark** to add them to your audit. McAfee recommends that you use only one benchmark per audit.
4. Choose a profile for your audit: in Selected Benchmarks, select the profile from the Selected Profile drop-down list, then click **Next**.

   NOTE: Some benchmarks don't have profiles.

5. Choose a method for adding systems to the audit:
   - Select **System Tree and Tags** and click **Add System**, **Add Group**, or **Add Tag** to add systems to the audit. You can use more than one method to add systems.
   - Select **Criteria**, then select one or more **Available Properties** to add to the **Computer Properties** pane. Use arrows in the Available Properties pane to add or remove criteria and the Comparison and Value controls lists to type or select system properties.
6. Under the **Exclude these** pane, click **Add System** to exclude systems from the audit, then click **Next**. The **Properties** page appears.
7. Type audit information and select options, then click **Next**. The Summary page appears.
8. Review the information, then click **Save**.

Run an audit manually

You can manually run an audit when you need to view results before the next scheduled audit.

Task

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

1. Click **Menu | Policy | Audits**.
2. Select one or more audits, then click **Actions | Run Audit**.

The audit runs during the next whiteout period.

Disable an audit

You can disable an existing audit. When an audit is disabled, McAfee Policy Auditor continues to purge information according to the schedule you have set. The audit will not run until you re-enable it.

Task

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

1. Click **Menu | Policy | Audits**.
2. Select an audit, then click **Actions | Edit Audit**. The New Audit Builder opens.
3. Click **Next** to display the properties page.
4. Deselect **Enable this Audit**, then click **Next**.
5. The Summary page appears. Click **Save**.

Delete audits

You can delete an audit and all associated results and findings when you no longer need them.

Task

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

1. Click **Menu | Policy | Audits**.
2. Select the audits you want to delete and click **Delete**.

Audit whiteout and blackout periods

Audit whiteout periods are time intervals when an audit can run on a system or group of systems. Audit blackout periods are time intervals when an audit can not be run.

Audits are not scheduled. For example, consider a benchmark that was last evaluated at 5:14 p.m. on Sunday May 6th. The frequency requirement states the information should not be older than 4 days. Blackout windows are set from 8:00 a.m. to 5:00 p.m. on weekdays. Whiteout windows cover the remaining period.

If the benchmark is scheduled for re-evaluation during the Thursday evening whiteout window, the frequency requirement of 4 days is calculated so the benchmark must be evaluated no later than Thursday morning.

Audit content updates sent to the ePolicy Orchestrator server cause McAfee Policy Auditor to run the audit at the next available whiteout period.

NOTE: Agentless audits conducted by Foundstone or McAfee Vulnerability Manager do not honor whiteout and blackout periods.

Set whiteout and blackout periods

Set whiteout and blackout periods for running audits on systems.

Task

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

1. Click **Menu | Systems | System Tree** and select the **Assigned Policies** tab.
2. Select McAfee Policy Auditor Agent 6.0.0 from the **Product** drop-down list.
3. Under the **Actions** column, click *edit assignments*. The Policy Assignment page appears.
4. Under Assigned policy, click **Edit Policy**. The whiteout/blackout page appears. White squares represent periods of time when audits for the specified System Tree group are allowed to run. Blue squares represent periods of time when audits for the specified System Tree group are not allowed to run.
5. Click a white square, which changes the color to blue, to designate a period of time when audits are not allowed to run. Click a blue square, which changes the color to white, to designate a period of time when audits are allowed run.
6. Click **Save**.

Service Level Agreements

Service Level Agreements (SLAs) are relationships that you create between system tags and patch severity levels. You then specify a number of days that you have to apply patches to systems that fit the relationship.

As an example, you assign tags to systems, such as Finance or Administrative, to systems and check creators can assign severity levels, such as Critical or Moderate, to patch checks. When you create a Service Level Agreement, you can specify that Finance systems missing a Critical patch are given 30 days until you are required to apply the patch. Similarly, you can specify that Administrative systems failing a Critical patch check are be given 90 days before you are required to patch the System.

You can monitor the status of Service Level Agreements from the **PA: MS Patch Status Summary** dashboard monitor.

Create, edit, and delete Service Level Agreements

Create, edit, or delete a Service Level Agreement between a system tag and a patch severity.

Task

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

1. Click **Menu | Risk & Compliance | Audits**, then click **New SLA**. The Service Level Agreement page appears.
2. Click **New SLA**. The Add Service Level Agreement page appears.
3. Select a tag from the **Select A Tag** drop-down list. Select a severity level from the **Select A Severity** drop-down list.
4. Type the number of days that you have to install a patch after an audit discovers a system matching the tag that requires a patch matching the severity level. Click **Save**.
5. You can edit or delete a Service Level Agreement.

Option	Definition
Edit SLA	Edit the Service Level Agreement

Option	Definition
Delete SLA	Delete the Service Level Agreement

How viewing audit results works

McAfee Policy Auditor software offers a number of options for viewing audit results.

Several options are available for viewing system and rule compliance. You can view audit results by clicking an audit from the Audits page.

Results timeframe control

The **Results timeframe** control allows you to view the results of an audit at any point in time since the audit first began. By default, the calendar is set to **Today**, which shows the results for current systems as defined by the frequency settings. A checkbox is available to show the last valid results if today's results are not current. Finally, the calendar control allows you to pick a date in the past and see the audit results for that date.

Audit Benchmarks pane

The **Audit Benchmarks** pane shows the status of each benchmark in the audit. You can view these columns in the pane:

- **Benchmark ID** — Benchmark identifier.
- **Profile ID** — Profile identifier, if any.
- **Pass** — The number of benchmarks for which all systems passed the audit.
- **Fail** — The number of benchmarks for which all systems failed the audit.
- **pass-expired** — The results have expired but the last audit results evaluated to *pass*.
- **fail-expired** — The results have expired but the last audit results evaluated to *fail*.
- **other-expired** — The results have expired and the previous audit results evaluated to a condition other than *pass* or *fail*.

You can click on the hyperlinked number in the columns to take you to the View System Results page.

View System Results column

Under the **View Results** column, clicking **systems** allows you to view the results for each system audited. This is an extension of the Audit Results pane that allows you to see the results at the system level. These columns appear in the Benchmark Systems pane:

- **Audit Date** — The date of the audit being viewed.
- **Expiration Date** — The expiration date, if any, of the audit.
- **Score** — The audit score for the system.
- **System Group** — The name of the group, if any, that the system belongs to.
- **System Name** — The name of the system.
- **System Tags** — Any tags associated with the system.
- **Rules Passed** — The number of rules that passed the audit.
- **Rules Failed** — The number of rules that failed the audit.

- **Rules Other** — The number of systems that had a result other than *pass* or *fail*.

The page provides a control that allows you to view the results by system group, system subgroup, systems with a specific tag, or even individual systems.

You can also adjust the results timeframe to select an audit to review.

View Rule Results column

Under the **View Results** column, clicking **rule** allows you to view the rule results for each system audited. This is an extension of the Audit Results pane that it allows you to see the results at the rule level. These columns appear in the Benchmark Rules pane:

- **Rule ID** — The benchmark rule identifier.
- **Group Path** — The path of the group containing the rule.
- **Systems Passed** — The number of systems that passed the audit.
- **Systems Failed** — The number of systems that failed the audit.
- **Systems Other** — The number of systems that had a result other than *pass* or *fail*.

The page provides a control that allows you to view the results by benchmark rule group, benchmark rule subgroup, or a specific rule which can be selected by clicking **Find** and selecting a rule.

Exporting audits and audit results

Audits and audit results can be exported in two different formats: XCCDF and OVAL. In each case, the information is saved as a ZIP file. Common uses for exporting audits is for transfer to another ePolicy Orchestrator server or for use in a third-party application.

Option	Definition
Export XCCDF	Creates an XCCDF file that conforms to the XCCDF results schema. It contains the latest results for all the systems and benchmarks in the audit. The results file could be consumed by any tool that understands the XCCDF results schema.
Export OVAL	Creates an OVAL results file that conforms to the OVAL results schema. This file can be consumed by any tool that understands the OVAL results schema. For example, Remediation Manager 4.5 can import OVAL results.

Export audits

Export an audit to a file that conforms to the XCCDF or OVAL results schema.

Task

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

1. Click **Menu | Risk & Compliance | Audits**.
2. Select the audit to export and click one of these options.

Option	Definition
Actions | Export XCCDF	Export an audit to a file that conforms to the XCCDF results schema.
Actions | Export OVAL	Export an audit to a file that conforms to the OVAL results schema.

3 The File Download dialog box appears. Click **Save.** The Save As dialog box appears.

4 Give the export ZIP file an appropriate name and click **Save**.

Scoring Audits

When McAfee Policy Auditor performs an audit on a system, it generates information about system compliance that includes a compliance score.

The software supports the four scoring models described in the National Institute of Standards and Technology (NIST) document Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.1.4 (http://csrc.nist.gov/publications/nistir/ir7275r3/NISTIR-7275r3.pdf):

- Default scoring model
- Flat unweighted scoring model
- Flat scoring model
- Absolute scoring model

The software is preconfigured to use a normalized implementation of the flat unweighted score model. You can change the scoring model and the software recalculates scores to reflect the change.

Contents

Default scoring model

The default scoring model computes the score independently for each collection of subgroups and rules in each group, and again for each rule and group within the audit's benchmark(s).

Despite the name of the scoring model, McAfee Policy Auditor does not use this model for its preconfigured scoring model. Instead, the software uses a normalized version of the flat unweighted scoring model that makes it easier to compare audit scores.

Calculating scores using the default scoring model

The calculated test score under the default scoring model depends upon the number of groups, subgroups, and rules in benchmarks within an audit. This means that audits containing large benchmarks can yield a high score while audits containing small benchmarks can yield a low score. Audits can also have rules that are based on the system configuration, so it is possible, for example, for the same audit to yield one score on an Windows XP system and another score on a Windows 7 system.

Since the maximum possible score can vary from audit to audit and from system to system, it is difficult to compare audit scores. The primary use for this scoring model is for comparing historical audit scores on the same system.

Flat unweighted scoring model

The flat unweighted scoring model computes the score (the number of rules that passed) and compares it against the maximum possible score. McAfee Policy Auditor is preconfigured to use a normalized implementation of the flat-unweighted score model.

The maximum possible score is the number of all applicable rules in an audit. For example, if an audit evaluates a system against 283 rules and the system passes 212 of the rules, the flat unweighted scoring model gives the system a score of 212. Another audit might have fewer rules and yield a lower score. This makes it difficult to compare results from different audits.

How McAfee Policy Auditor calculates scores

Because of the disparity in comparing audit scores, the software is preconfigured to use the flat unweighted scoring model and normalize the final score to a maximum possible score of 100. This allows you to reliably compare an audit with other audits on the same system or between systems with different configurations, such as Windows XP or Windows 7.

The software uses this equation to normalize audit scores:

audit score = (rules passed ÷ maximum possible score) × 100

This table shows how scores for different audits can be compared using a normalized implementation of the flat unweighted score model.

Audit example	Maximum possible score	Rules passed	Flat unweighted audit score	Normalized flat unweighted audit score
Audit 1	283	212	212	74.9
Audit 2	15	14	14	93.3

Flat scoring model

The flat scoring model compares the system score with the maximum possible system score.

The maximum possible score is the sum of the weights of all rules in an audit that apply to a system. Rules that do not apply to a system are ignored when calculating the maximum possible score. The actual score is the sum of the weight of all rules that pass.

Since the maximum possible score can vary from system to system, scores from systems that have different configurations, such as Windows XP or Windows 7, may not be directly comparable. This model is useful for comparing a system score with its historical scores.

Score weighting

The flat scoring model allows benchmarks to use weighted scores for each rule. A common example of score weighting is a school test where one question is worth more points than another question.

In this example, an audit has a benchmark with two rules. One of the rules is weighted because the audit benchmark developer considered it to be more important than the other rule.

Rule	Assigned weight	Laptop maximum rule score	Non-laptop maximum rule score
Port 8015 on a laptop system is closed	3	3	0
Password on any system must be 10 or more characters	1	1	1
Maximum possible score		**4**	**1**

The maximum possible audit score for a laptop is 4. On desktop systems, the software ignores the closed port rule and the maximum possible score is 1.

Absolute scoring model

The absolute scoring model yields a score of 100 when a system passes all applicable rules, and a score of 0 if all applicable rules do not pass.

This scoring model is useful when an organization requires that a system pass every rule to be considered secure. The absolute scoring model makes it easy to differentiate between systems that pass or fail an audit.

Changing the scoring model

You can change the scoring model that McAfee Policy Auditor uses when reporting audit results. When you change the scoring model, the software recalculates the scores to reflect the selected model.

Before you begin

You must have appropriate permissions to perform this task.

Task

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

1. Click **Menu | Configuration | Server Settings**.
2. Under **Setting Categories**, select **Policy Auditor**. The McAfee Policy Auditor server settings appear in the right panel.
3. Click **Edit**. The Edit Policy Auditor page appears.
4. Select the scoring model from the **Default Scoring Model** drop-down box.
5. Click **Save**.

Managing Audit Waivers

Waivers allow you to temporarily affect how systems are audited and have the potential to affect audit scores. They are useful when you have a system that you know may be out of compliance but you do not want to bring the system into compliance for a temporary period.

For example, you may have systems in the Accounting Department that you do not want to patch near the end of an accounting cycle. You can create a waiver that will temporarily ignore any missing patches on systems until after the end of the accounting cycle. You can also create another type of waiver that suppresses the systems from being audited.

Contents

Types of waivers

McAfee Policy Auditor provides three types of audit waivers that apply to selected systems. Each type of waiver affects scoring results differently:

- **Exception waiver** — Forces the audit results of a selected benchmark rule to have a result of *pass*. This potentially affects the score of system audits.
- **Exemption waiver** — Prevents selected systems from being audited. Systems not audited do not appear in audit results.
- **Suppression** — Allows a selected benchmark rule to be included in an audit, but excludes the results. This affects the score of system audits.

All waivers have these common characteristics:

- A system, multiple systems, or groups of systems selected from the System Tree.
- A start date and an expiration (end) date.

In addition, exception and suppression waivers must include a selected rule from a selected benchmark. The waiver applies to any audit that contains the benchmark. Since exemption waivers are independent of benchmarks or rules, the interface does not give you the opportunity to select them.

Exception waivers

Exception waivers potentially affect the audit scores of selected systems by forcing the audit result of a benchmark rule to have a status of *pass*. The primary use of an exception waiver is to force audit rules to pass.

Exception waivers have these characteristics:

- They apply to selected systems and groups in the System Tree.
- They require you to select an audit benchmark and a rule contained in the benchmark.
- They evaluate every rule during an audit, but force the selected rule(s) to have a status of *pass*.
- They can be backdated. Scores for results collected during the backdate timeframe are recalculated.

For example, McAfee Policy Auditor audits a system with a benchmark that contains five rules. Four rules pass and one fails, resulting in a score of 80%. If the rule that failed is granted an exception waiver, all five rules are considered to have passed and the score is 100%.

Exemption waivers

Exemption waivers prevent selected systems from being audited.

Exemption waivers have these characteristics:

- They apply to selected systems and groups in the System Tree.
- They do not require you to select a benchmark and a rule.
- They cannot be backdated.
- They do not audit the selected systems when the waiver is in effect.
- They do not include selected systems in the audit results.

For example, McAfee Policy Auditor audits a system with a benchmark that contains five rules. Four rules pass and one fails, resulting in a score of 80%. If the system is granted an exemption waiver, it is not audited and does not appear in the audit results.

Suppression waivers

Suppression waivers potentially alter the audit scores of selected systems by excluding the audit result of a benchmark rule. The primary use of a suppression waiver is to hide the audit results.

Suppression waivers have these characteristics:

- They apply to selected systems and groups in the System Tree
- They require you to select an audit benchmark and a rule contained in the benchmark.
- They evaluate every rule during an audit, but do not include the rule result when calculating the score.
- They can be backdated. Scores for results collected during the backdate timeframe are recalculated.

For example, McAfee Policy Auditor audits a system with a benchmark that contains five rules. Four rules pass and one fails, resulting in a score of 80%. If the rule that failed is granted a suppression waiver, the rule results are excluded and the score is 100%.

Waiver status

Waivers can have one of four status properties.

Status	Description
Requested	A waiver has been requested but approval has not been granted for it to take effect. Requested waivers do not appear on the **Waivers** tab, but appear in the **Issue Catalog** (go to **Menu | Automation | Issues**). Requested waivers can be deleted.
Upcoming	A waiver has been requested and granted approval but the waiver is not in effect because the start date has not yet arrived. Upcoming waivers can be deleted.
In-effect	A waiver is active and audits involving the system specified by the waiver temporarily affect the scoring of the system. In-effect waivers cannot be deleted but can be cancelled to give it a status of *expired*.
Expired	A waiver is no longer in effect, because of user intervention or the expiration date has arrived. Expired waivers cannot be deleted.

Filtering waivers by status

You can filter waivers by their status.

Task

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

1. Click **Menu | Risk & Compliance | Waivers**.
2. Select a group from the System Tree containing waivers of different status.
3. Use the **Status** drop-down list to select a status. The software filters waivers based upon your choice.

How start and expiration dates work

Waivers are effective for a limited time only. When you create a waiver, you specify a start date and an expiration date.

The start date is when the waiver takes effect. The expiration date is when the waiver is no longer in effect. The start date is inclusive and the expiration date is not inclusive.

The expiration date must be at least one day after the start date.

For example, if you set a start date of March 1, 2013 and an expiration date of April 1, 2013, the waiver affects audits from March 1, 2013 through March 31, 2013. An audit conducted on April 1, 2013 is not affected by the waiver.

Examples of filtering waivers by date

When you filter waivers by date, McAfee Policy Auditor shows waiver status as of the selected date. The status may change according to the date you select for filtering.

These assumptions apply to the filtering examples:

- Today's date is November 10, 2012.
- Waiver A has a start date of November 1, 2012 and an expiration date of November 15, 2012.
- Waiver B has a start date of November 15, 2012 and an expiration date of December 1, 2013.

Filter by today's date

Next to the **As of** date, click **Today**. The date is set to today's date of November 10, 2012. The Waivers tab shows:

- Waiver A has a status of *In-effect*.
- Waiver B has a status of *Upcoming*.

Filter by a future date

Next to the **As of** date, select November 15, 2012. The Waivers tab shows:

- Waiver A has a status of *Expired*.
- Waiver B has a status of *In-effect*.

Filter by a past date

Next to the **As of** date, select October 1, 2012. The Waivers tab shows:

- Waiver A has a status of *Upcoming*.
- Waiver B has a status of *Upcoming*.

Filtering waivers by date

McAfee Policy Auditor allows you to filter waivers according to a date that you select.

Task

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

1. Click **Menu | Risk & Compliance | Waivers**.
2. Use the calendar control next to **As of** to select a different date.

The Waivers tab shows the status of each waiver as of the selected date.

Filtering waivers by group

McAfee Policy Auditor allows you to filter waivers by the group selected in the System Tree.

Before you begin

You must have a group with a subgroup that contains waivers.

Task

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

1. Click **Menu | Risk & Compliance | Waivers**.
2. Select the group containing the waivers from the System Tree.
3. From the **Filter** drop-down list, select **This Group Only**. The waivers tab shows only the waivers for systems in the selected group.
4. Select **This Group and all Subgroups** from the **Filter** drop-down list.

The Waivers tab shows waivers for systems in the selected group and any subgroups of the selected group.

How waiver requests and grants work

McAfee Policy Auditor software shows waivers on the Waivers page when a user with the proper permissions grants approval for the waiver to take effect.

Depending upon the internal security policies of your organization, the users who request waivers and the users who grant them can be different. A user who has permissions to request and grant waivers can create a waiver and grant it at the same time.

Requesting waivers

McAfee Policy Auditor software allows you to request a waiver. If a user only has permissions to request waivers, another user who has permissions to grant waivers must grant the waiver before it appears on the Waivers page. If you have the correct permissions to grant waivers, you can create and grant the waiver in a single step.

Requested waivers appear in the Issues Catalog.

Before you begin

You must have permissions to request waivers.

Task

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

1. Click **Menu | Risk & Compliance | Waivers**, then click **New Waiver**. The Waiver Request page appears.
2. Type a name for the waiver. In the **Notes** box, type descriptive information that you want to associate with the waiver.
3. From the **Waiver Type** drop-down list, select the type of waiver that you want to create.
4. Use one or both of these options to select systems to apply the waiver to:
   - Click **Add Systems**. The Quick System Search dialog box appears. Type the system name, IP address, MAC address, or user name that you want to search for. If you do not know the full name or address, you can type a partial search, like 172.21. Click **OK**. The Search Results page appears.
   - Click **Add Group**. The Select Tree Group dialog box appears. Select a group from the System Tree and click **OK**. Repeat as needed.
5. Select the systems that the waiver applies to, then click **OK**. The Waiver Request page appears.
   - For exception and suppression waivers, select a benchmark and one or more rules.
   - Exemption waivers do not require a benchmark and a rule.

6 Use the calendar control next to the **Start Date** and an **Expires Date** to select dates for the waiver to be in effect. The **<** and **>** controls move the month backward and forward. The **<<** and **>>** controls move the year backward and forward.

7 Click **Request Waiver**. The Waivers tab appears. The requested waiver does not appear in the Waivers tab because the waiver had not been granted yet. Requested waivers appear in the Issues Catalog (**Reporting | Issues**). If you have permissions to grant waivers, you can click **Grant Waiver** and the waiver will appear in the Waivers tab.

Granting waivers

Users with the permission to grant waivers can approve waivers requested by others.

Before you begin

You must have permissions to grant waivers.

Task

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

1 Click **Menu | Automation | Issues**.

2 Select a requested waiver and click **Edit**. The Edit Issue page will appear.

3 Click **Grant Waiver**.

The waiver is now approved to take effect on the start date.

Making waivers expire

You can make a waiver expire. This is useful when you have a waiver with a status of *In-effect* and you want to end the waiver before the expiration date.

Before you begin

You must have permissions to grant waivers.

Task

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

1 Click **Menu | Risk & Compliance | Waivers**. The Waivers tab appears.

2 Select a waiver with a status of *In-effect* and click **View**.

3 Click **Expire Waiver**.

The waiver has a status of *Expired*.

Deleting waivers

You can delete a waiver before it takes effect. You can only delete waivers with a status of *Upcoming*.

Before you begin

You must have permissions to grant waivers.

Task

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

1. Click **Menu | Risk & Compliance | Waivers**. The Waivers tab appears.
2. Select a waiver with a status of *Upcoming* and click **View**.
3. Click **Delete Waiver**.

The deleted waiver no longer appears on the Waivers tab.

File Integrity Monitoring and entitlement reporting

File integrity monitoring notifies you of changes to specified text files on managed systems. Entitlement reporting informs you of changes to user and group rights to files.

These features are useful for complying with government and industry standards, such as the Payment Card Industry (PCI) Data Security Standard.

Contents

How file integrity monitoring works

The file integrity monitoring feature uses the McAfee Policy Auditor agent plug-in to track file changes to specified text files.

The software monitors files on managed systems only. You must install the McAfee Agent and the agent plug-in on systems that you monitor.

When a file is scanned, the agent plug-in returns an event to the McAfee Policy Auditor server. The event is encrypted and compressed to save disk space and bandwidth.

To learn more about supported systems, see:

- *Managed Systems* in the *Using the McAfee Policy Auditor agent plug-in* section.
- *Platforms supported by the McAfee Policy Auditor agent plug-in* in the *Using the McAfee Policy Auditor agent plug-in* section.

When you create a policy to monitor files, the software checks the file for changes every hour by default. You can change the monitoring frequency to fit your organizational needs.

File integrity monitoring allows you to:

- Define which files should be tracked. You can use wildcard characters in file and path names.
- Define which files should not be tracked.
- Specify the frequency for detecting file changes.
- See and receive notification about changes to the file or file attributes.

McAfee Policy Auditor also provides the ability to retain up to six file versions, including the baseline version, and provides the ability to:

- Compare a file with it's baseline version, or any prior version.
- Compare a file with a file on another system.

- Show a side-by-side comparison of file changes and indicate which lines have been added, deleted, or modified.

File information monitored

The file integrity monitoring feature of McAfee Policy Auditor tracks a number of file attributes. A change in an attribute generates an event notifying you of the change.

The monitored attributes differ between the various supported operating systems.The software monitors these attributes on all operating systems.

- File size (in bytes)
- File created (date and time)
- Last modified (date and time)
- Read only
- Hidden
- System
- Owner
- Group

On Windows systems, the software monitors these attributes, the Archive attribute, plus permissions from the Discretionary Access Control List (DACL)

File baselines

When you create and apply a policy, the agent plug-in scans the file to create a baseline. The baseline contains information about the file attributes, and contains the file text if file versioning is enabled.

If the file is changed, the software generates an event that is logged to the File Integrity Monitor page, included in reports, and can be handled by the issues and tickets feature of ePolicy Orchestrator software software.

McAfee Policy Auditor software monitors the MD5 and SHA-1 hashes of a file as well as the file attributes and permissions information. These values are stored in a database that is created on each system and on the software server.

Each time the file is scanned, the software compares its configuration to the baseline. When the file or an attribute changes, the agent plug-in detects the change and sends an event back to the server according to the monitoring frequency. If versioning is enabled, the text file contents are sent to the server as well.

Reset file baselines

You can create a new baseline for all monitored files on a system from the Systems tab of the File Integrity page. You can also accept file integrity monitoring events, which creates a new baseline for the selected file and discards old baseline versions.

Monitored and excluded files

You can create a policy to monitor file changes on a regular schedule. The interface allows to specify files to monitor and files to exclude from monitoring. It also provides the capability to monitor subfolders under each specified path and to monitor symbolic links.

Wildcard characters

Monitored and excluded paths and file names support the ***** and **?** wildcard characters. The ***** wildcard character represents one or more characters and the **?** wildcard represents a single character.

You can choose to monitor a single file by typing the name of the file when you create a file integrity monitoring policy. By using wildcard characters, you can monitor files or paths of a specific type. For example, if you type ?:\Config for the path and *.txt for the file, McAfee Policy Auditor monitors all text files in the Config folder on all hard drives. You can exclude specific paths and files in a similar manner.

File validation

McAfee Policy Auditor does not validate the existence of files. It ignores paths or files that do not exist.

File versioning

McAfee Policy Auditor allows you to store up to six versions, including the file baseline, of text files from managed systems. The software does not support versioning for non-text files.

NOTE: The actual text files are not stored in the software database. The database stores the text file contents for quick comparison purposes, even when the system is not connected to the network.

When you create a policy, you have the opportunity to store file versions for comparison purposes. The number of file versions you can store ranges from 2 to 6. This number includes the baseline version.

File versions are stored on a First In, First Out (FIFO) basis. For example, if you configure the software to store 3 versions, it stores the baseline version plus the two most recent versions. If the file changes, the oldest non-baseline file is purged to recover disk space by an internal server task that runs once a day by default.

Configuring the maximum number of stored file versions

When you create a file integrity monitoring policy, you can specify the maximum file size stored for each version with the **Max versioned file size** setting. The available settings range from 1 to 4 MB.

For example, if you set **Max versioned file size** to 3 MB, the text in the file is stored when its size is less than or equal to 3 MB. If the file size exceeds 3 MB, the software alerts you with an error message. If you receive an error message, you can edit the policy so that it stores text from files as large as 4 MB.

Configuring the maximum number of file integrity monitoring files

You can configure how many versions of files are stored by the software. Use the Server Settings page to set the number of file versions stored by McAfee Policy Auditor. For more information, see *Max number of FIM version files* and *Edit Server Settings* in the *Getting Started with McAfee Policy Auditor Software* section.

File version comparison

The comparison feature allows you to view the contents of a versioned file and compare the text file content with other files. The software uses a color-coding system to identify file lines that are equal, empty, deleted, inserted, or modified.

You can compare a stored version of the text with:

- The file baseline.
- Previous file versions.
- A specified file on another system.

Double-byte characters

The file version comparison feature supports files containing only single-byte characters in the filename and contents. It does not support file comparison for files containing double-byte characters.

Accept file integrity monitoring events

When a monitored file changes, it generates an event that you can accept.

You can accept one or more events from the File Integrity page or from pages that you drill down to in reports:

- Accepting an event designates the changed file as the new baseline version and purges, or deletes, any previous versions.
- Accepting multiple events designates the most recently changed files as the new baseline version and purges any previous version.
- Accepting an event for a versioned file sets it as the new baseline version and purges previous versions of the file.

You can also accept events from the file integrity monitoring query reports drilldown pages.

Purge file integrity monitoring events

You can purge, or delete, file integrity monitoring events. The software purges events based on a selected age. You can also choose to purge baseline events.

Purging events does not set a new baseline. If you select the option to purge baseline events on a versioned file, you cannot compare later files with the purged baseline file. However, you can compare file versions that have not been purged.

If you purge a baseline file, the software discards the stored baseline file information, including stored text if versioning is enabled. The software retains the baseline file hash information and sends events with new file information when the file changes.

You can also purge events from the last page shown when you drill down into file integrity monitoring query reports.

Entitlement reporting

Entitlement reporting informs you of changes to user and group rights to files. Changes to a file's access permissions entitlement generates an event notifying you of the change.

One aspect of compliance monitoring is knowing which accounts have access to which files. McAfee Policy Auditor monitors these access permissions.

- User — User who has access to the file.
- Is Group — Whether the User is a group.
- Read Data — Whether the User has the ability to read the file.
- Write Data — Whether the User has the ability to write to the file.
- Execute — Whether the User has the ability to execute the file.
- Delete — Whether the User has the ability to delete the file.

Create and apply a file integrity monitoring policy

Using a file integrity monitoring policy is a two-stage process. First, you must create the policy. Next, you must apply the policy to selected systems in a System Tree group. You can create one policy per group.

Tasks

- Create a file integrity monitoring policy
- Apply a policy to systems
- Compare file versions
- Accept file integrity monitoring events
- Purge file integrity monitoring events
- Create a new file integrity monitoring baseline

Create a file integrity monitoring policy

Create a policy to monitor file integrity, file entitlement, and version changes.

Before you begin

You must install the McAfee Policy Auditor agent plug-in on all systems that are to be monitored. For instructions on how to do this, see *Managing the McAfee Policy Auditor agent plug-in*.

When adding, editing, or excluding text files, you can use the **?** wildcard to represent one character and the ***** wildcard to represent multiple characters.

Task

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

1. Click **Menu | Policy | Policy Catalog**.
2. From the Product drop-down list, select **Policy Auditor Agent 6.0.0**.
3. From the Category drop-down list, select **File Integrity Monitor**.
4. Click **Actions | New Policy**. The New policy dialog box appears.
5. Provide information about the new policy:

Option	Definition
Category	Select File Integrity Monitor. This is selected by default.

Option	Definition
Create a policy based on this existing policy	Select an existing policy, such as My Default, or another file integrity monitoring policy.
Policy Name	Type a meaningful name for the policy
Notes	Type information about the policy. This field is optional.

6 Click **OK.** The policy configuration window opens. Use the three tabs to configure the policy.

Table 1: Monitor tab

Use this:	To do this:
Add	Open the Monitor Item dialog box: • **File path** — Type a file path to the monitored file(s). • **File name** — Type a file name to monitor, using wildcard characters as needed. • **Include subfolders** — Monitor files in subfolders of the file path. This is useful when you use wildcard characters in file names. • **Follow symlinks** — Monitor files referenced by symlinks or shortcuts in the file path. • **Monitoring setting** • **File Entitlement** — Monitors whether a file has changed. • **File Entitlement, File Integrity** — Monitors whether a file has changed or whether the file's entitlements have changed. • **File Entitlement, File Integrity, File Versioning** — Monitors whether a file has changed, whether the file's entitlements have changed, and stores changes for supported text files .
Edit	Change the configuration of the selected file.
Max versioned file size (1-4 MB)	Select the maximum size of the files in the policy. You can only use versioning on text files. This has no effect on files that do not have versioning enabled.
Remove	Remove the selected file from the list of files to be monitored.

Table 2: Exclude tab

Use this:	To do this:
Add	Open the Exclude Item dialog box: • **File path** — Type a file path to the file(s) you want to exclude from monitoring. • **File name** — Type a file that you want to exclude from monitoring. This is useful when you use wildcard characters for monitored files.
Edit	Change the configuration of the selected file.

Use this:	To do this:
Remove	Remove the selected file from the list of files to be monitored.

Table 3: General tab

Use this:	To do this:
Run every	Set the monitoring frequency for the file. By default, this is set to one hour.

7 Click **Save**.

Apply a policy to systems

When you create a file integrity monitoring policy, you can apply it to systems in a selected System Tree group. You can apply one file integrity monitoring policy to a group.

Task

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

1 Click **Menu | Systems | System Tree**.

2 Select the System Tree group that you want to apply the policy to.

3 From the Systems tab, select the systems that you want to apply the policy to.

4 Select the **Assigned Policies** tab, From the **Product** drop-down list, select Policy Auditor Agent 6.0.0.

5 Click **Edit Assignment** for a policy with a category of File Integrity Monitor. Under the **Actions** column heading, click **Edit Assignment**. The Policy Assignment page appears.

6 Select **Break inheritance and assign the policy and settings below**.

7 In the **Assigned policy** drop-down list, select a file integrity monitoring policy.

- Click **Edit Policy** to make changes to the policy.
- Click **New Policy** to create a new policy based on the selected policy.

8 Lock or unlock policy inheritance based on your needs. If you lock inheritance, you will not be able to create a new policy based upon this policy that breaks inheritance. McAfee recommends that you unlock policy inheritance for file integrity monitoring policies. Click **Save**.

Compare file versions

When you enable file versioning, you can compare a file with a previous version, the baseline file, or a file on another system.

Task

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

1 Click **Menu | Reporting | File Integrity**, then select the **Events** tab.

2 Select a versioned file event, then click **Actions | Compare**. The Select two files for comparison page appears.

3 The file in the File 1 pane is the file you selected. You can use the **File name** drop-down list to select another file and the Version drop-down list to select a different file version. Click **Preview** to see the file contents.

4 Select the options for the File 2 paneL

Use this....	To do this
Compare with the baseline on the above host	Compare the file in the File 1 pane to the baseline version.
Compare with the previous version on the above host	Compare the file in the File 1 pane to the previous file version.
Select a file	Select another file for comparison on the system or another system: • **Host** — Opens the Quick System Search dialog box. Select the file on the Search Results page and click **Select**. • **File name** — A versioned file on the selected host. • **Version** — A version of the selected file.

5 Click **Run Comparison**. The File Comparison page appears.

Use this....	To do this
Show/Hide Attributes	Show or hide the file attributes.
Context Size	Sets the number of lines to show surrounding lines from the empty, deleted, inserted, or modified lines in File 2.

Accept file integrity monitoring events

McAfee Policy Auditor generates events when monitored files change. You can accept events and automatically create a new file baseline.

Task

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

1 Click **Menu | Reporting | File Integrity**, then select the **Events** tab.

2 Select the file events to accept, then click **Actions | Accept**.

Purge file integrity monitoring events

McAfee Policy Auditor generates events when monitored files change. You can purge events based on their age.

Task

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

1 Click **Menu | Reporting | File Integrity**, then select the **Events** tab.

2 Select the file events to purge, then click **Actions | Purge**. The Action: Purge dialog box appears.

3 Edit the dialog box to purge events older than the specified time. Select **Purge Baseline Events** to discard stored baseline settings, including the file text if versioning is enabled. Click **OK**.

Create a new file integrity monitoring baseline

You can create a new file integrity monitoring baseline for all monitored files on a system.

NOTE: Use the Accept command on the File Integrity Events page to accept events for one or more files and automatically create new baselines.

Task

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

1 Click **Menu | Reporting | File Integrity**, then select the **Systems** tab.

2 Select a system, then click **Actions | Reset Baseline**. The reset baseline dialog box appears. Click **Yes**.

Query reports for file integrity monitoring

McAfee Policy Auditor software provides four built-in query reports for file integrity monitoring.

Each report provides information on events and allows you to drill down to see detailed information. The query reports also allow you to accept or purge events and to compare file versions if file versioning is enable. You can edit the queries, make new queries based on the existing queries, and add the queries to a dashboard.

PA: File Integrity - All Events

Displays an aggregated count of file integrity events grouped by the associated baseline date.

PA: File Integrity Event Counts

Displays a pie chart of file integrity events grouped by event type.

PA: File Integrity Events By System/Baseline Date

Displays a list of the file integrity exceptions encountered after a baseline reset, grouped by system and baseline date.

PA: File Integrity Events By System/Event Type

Display a an aggregated count of file integrity events grouped by system.

Rollup reporting

You can run queries that report on summary data from multiple ePolicy Orchestrator databases. McAfee Policy Auditor can use this feature to create rollup reports for audit results.

Contents

Rollup capabilities

You can roll up three types of audit information from multiple servers.

The software provides rollup capabilities for these areas of audit information:

- Benchmark results
- Rule results
- Check results, including patches

Each of these areas is independent and any combination of the three can be rolled up. You can include information from each of the areas because the data is related.

Rollup reporting considerations

You should carefully plan your rollup reporting configuration before implementing the feature.

Here are some issues to consider:

- The volume of audit results can be substantial. Care should be given to only roll up essential data. This is especially true for rules and checks.
- The actual time to complete the initial roll up reporting run will vary based on the amount of data in the source databases. Future runs will take less time if performed at frequent intervals. If the sources have a large amounts of data the roll up process may take several hours to complete. Each time the roll up server tasks are run, they appear in the Server Task Log to show the status of the process.
- When creating reports, only include data that is being rolled up. Otherwise results may not be accurate. For example, if only rule results are being rolled up by a server task, do not include benchmark results in the report because it will not contain data.

Rollup server tasks

McAfee Policy Auditor includes three predefined server tasks to provide rollup reporting. The tasks are disabled by default.

The tasks can roll up information to provide a meaningful view of audit results from multiple servers. The server tasks have predefined settings that do not limit the data returned. You can configure the settings by editing the tasks from the server tasks page.

Rollup Data - PA: Audit Benchmark Results

This task rolls up benchmark results and its associated database tables.

Data rolled up	Actions
Audit Benchmark Result Score Rollup	• **Purge** • No purging • Purge all • Purge rolled up items older than a specified period of time • **Filter** • Score • Scoring system • Audit end time • Audit expiration date • Audit name • Benchmark name • Benchmark profile • Is most recent result • System name • Waiver in effect • **Rollup method** • Incremental • Full
Benchmark Text Rollup	• **Purge** • No purging • Purge all • **Filter** (none available) • **Rollup method** • Incremental • Full
Benchmark Version Rollup	• **Purge** • No purging • Purge all • **Filter** (none available) • **Rollup method** • Incremental • Full

Rollup Data - PA: Audit Rule Result

This task rolls up audit rule results and its associated database tables.

Data rolled up	Actions
Audit Rule Result Rollup	• **Purge** • No purging • Purge all • Purge rolled up items older than a specified period of time • **Filter** • Benchmark group name • Benchmark L1 group name • Benchmark parent group • Group path • Rule name • Rule result • Waiver type • **Rollup method** • Incremental • Full
Benchmark Text Rollup	• **Purge** • No purging • Purge all • **Filter** (none available) • **Rollup method** • Incremental • Full
Group Text Rollup	• **Purge** • No purging • Purge all • **Filter** (none available) • **Rollup method** • Incremental • Full
Group Tree Rollup	• **Purge** • No purging • Purge all • **Filter** (none available) • **Rollup method** • Incremental • Full

Rollup Data - PA: Audit Patch Check Result

This task rolls up audit rule results and its associated database tables.

Data rolled up	Actions
Audit Check Result Rollup	• **Purge** ◦ No purging ◦ Purge all ◦ Purge rolled up items older than a specified period of time • **Filter** ◦ Check ID ◦ Check result ◦ Check status ◦ Check type (Default filter: Check type = Patch) • **Rollup method** ◦ Incremental ◦ Full
Audit Check Definition Rollup	• **Purge** ◦ No purging ◦ Purge all • **Filter** (none available) • **Rollup method** ◦ Incremental ◦ Full
Audit Check Text Rollup	• **Purge** ◦ No purging ◦ Purge all • **Filter** (none available) • **Rollup method** ◦ Incremental ◦ Full
Group Tree Rollup	• **Purge** ◦ No purging ◦ Purge all • **Filter** (none available) • **Rollup method** ◦ Incremental ◦ Full

Rollup reports

McAfee Policy Auditor comes with a number of predefined rollup reports. You can use these reports or use them as starting points to create new reports to fit your organizational needs.

The predefined reports show different aspects of audit results and use aggregation and grouping to help you interpret the information. You can drill down into each of the reports to find more detailed information.

- **PA Rollup Audit Rule Results Pass-Fail-Other** — Shows audit rules by status.
- **PA Rollup Benchmark Results - Failed by Scoring Category** — Shows benchmark results, categorized by scoring category, where the system failed the audit benchmark.
- **PA Rollup Benchmark Results - Pass-Fail-Unknown** — Benchmark results categorized as pass/fail/unknown.
- **PA Rollup Benchmark Results - Pass-Fail-Unknown by Server** — Benchmark results categorized as pass/fail/unknown, grouped by server.
- **PA Rollup Failed Audit Rule Results By Rule** — Displays failed audit results grouped by rule title and rollup server.
- **PA Rollup Failed By Actual Result, Benchmark, Group, Server** — Displays the actual results of a rule that failed during an audit. Data is grouped by server, benchmark, benchmark group and actual result. The average score is also displayed.
- **PA Rollup Failed Rules By Group And Server** — Displays the rules that failed when audited, grouped by benchmark group and server.
- **PA Rollup Patch Compliance Grouped by Server and Status** — Displays the rolled up patch compliance status grouped by server and status. Counts reflect the number of patches in the status.
- **PA Rollup Patch Compliance Overview** — Displays the rollup count of patches grouped by compliance status.
- **PA Rollup Patch Status by Benchmark, Server and Status** — Displays the rollup patch status grouped by benchmark, server, and status.
- **PA Rollup Patch Status by Status, Benchmark, and Server** — Displays the rollup patch status grouped by status, benchmark, and server.
- **PA Rollup Patch Status Grouped by Benchmark, Status and Server** — Displays the rollup patch status grouped by benchmark, server, and status.
- **PA Rollup Patch Status Grouped by Server and Status** — Displays the rollup of patch status grouped by server and status.
- **PA Rollup Patch Status Grouped by Status and Server** — Displays patch status grouped by status and server.
- **PA Rollup Rule Results By Result and Server** — Displays rules results that have been reported, grouped by result and server.
- **PA Rollup Rule Results By Server and Result** — Displays the audit rule results grouped by each rollup server.

Configure rollup reporting

Configure rollup reporting on a server to collect summary information from multiple servers.

Task

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

1. Set up your servers according to the *Multi-server rollup querying* section in your ePolicy Orchestrator Product Guide. Register each server with the reporting server.

2 Configure and enable these server tasks on each server, including the rollup server:

- Rollup Data - PA: Audit Benchmark Results
- Rollup Data - PA: Audit Rule Result
- Rollup Data - PA: Audit Patch Check Result

3 Configure and enable the *Roll Up Data (Local ePO Server)* server task on the reporting server.

Findings

Findings supplement the results of an audit check with additional information about the state of the machine.

Instead of seeing a value of *false* for a test result, Findings give more meaningful information such as "The minimum password length is set to 6 but it should be set to 8 or higher."

Contents

How findings work

McAfee Policy Auditor reports Findings, which are enhanced results, for supported checks. Findings appear in interface pages and queries and include additional information about why a system failed a check.

The software is installed as a separate extension called Findings and is exposed to McAfee and third-party applications through a Java API. This allows other applications to:

- Report additional details about Findings.
- Perform custom actions on Findings such as remediation on violations.
- Waive or hide selected Findings.
- Ignore Findings results.

Findings can include three types of information:

- **Violations** — Reporting violations provide additional information in audit results. For example, if an audit expects a password with at least 8 characters but finds a password with only 6 characters, the results show the actual and expected results. Since it is possible to create a check that reports thousands of violations. The software allows you to set a violation limit that reduces the number of violations that can be displayed to conserve database resources. Setting the violation limit to 0 causes monitors and queries to display all violations.
- **Compliant** — A message displayed when the system complies with the audit.
- **Incomplete** — A message displayed when the results gathered are not complete because they exceed the violation limit.

Types of violations

Violations are one of the types of information that can be shown by Findings. Violations can be one of three subtypes.

Types of violations

McAfee Policy Auditor shows information in reports and queries for three types of violations:

- **Positive feedback** — Additional information is shown when a rule passes. For example, if a rule determines whether the password age of a system is less than 90 days and the password is 60 days old, the enhanced results show that the expected value is <90 and the actual value is 60.
- **Violation with actual and expected values** — Additional information is shown when a rule fails. For example, if a rule determines whether the password of a system has 8 or more characters and the password has 6 characters, the enhanced results show a violation with the expected value of 8 and the actual value of 6.
- **Violation with instance data** — Additional information is shown for each instance of a violation, up to the violation limit. For example, if a rule asserts that folder *ABC* can only be accessed by administrators and the folder is shared, the enhanced results show every user that has access to the folder. If the number of users that have access to the folder is greater than the violation limit, then the additional violations do not appear in the report or query.

Violation limit

For some checks, failure can result in many violations. To save processing time, bandwidth, and disk space, McAfee Policy Auditor provides a violation limit that allows to cap the number of violations shown.

The violation limit sets the maximum number of violations that are created for a specific check. The default violation limit is 300. Setting the violation limit to 0 shows all violations.

You can change the violations shown globally through the system settings. You can also configure how violations are retained and purge through the use of per audit data maintenance, which allows you to override global system settings at the individual audit level.

Other Findings enhancements

Findings provide additional enhancements that improve the user experience.

McAfee Policy Auditor gives users the ability to:

- Import third-party Findings content, such as stylesheets and messages. You can import Findings content from the Checks page of McAfee Benchmark Editor.
- Hide or unhide Findings results.

Hide or unhide Findings results

You can hide or unhide selected Findings results for a failed check contained in an audit with at least one failed result.

Task

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

1. Click **Menu | Risk & Compliance | Audits**, then click an audit. The Audit Benchmarks page appears.
2. Click a number in the Rules Failed column. The System Rules - Failed page appears.
3. Under the Result column, click **fail** for a rule. The Rule Details page appears.

4 From the Checks pane, click **Results**. The Results page appears.

5 Select Findings that wish to hide or show.

Use this...	To do this...
Actions | Hide Findings	Hide Findings in reports for the check in this audit.
Actions | Unhide Findings	Show Findings in reports for the check in this audit.

Dashboards and Queries

Dashboards allow you to keep constant watch on your environment. Dashboards are collections of monitors, or reports. Monitors can be anything from a chart-based query, to a small web application, like the MyAvert Security Threats, that is refreshed at a user-configured interval.

You can create your own dashboards from query results or use the McAfee Policy Auditor default dashboards. Users must have the appropriate permissions to use and create dashboards.

Are you setting up dashboards for the first time?

When setting up dashboards for the first time:

1. Decide which default dashboards and default monitors you want to use.
2. Create any needed dashboards and their monitors, and be sure to make active any you want available as tabs from the navigation bar.

Refer to the ePolicy Orchestrator documentation for detailed information on how to build query reports that can be added to a dashboard.

Reporting queries and systems deleted from the system tree

McAfee Policy Auditor deletes audit results based on the policy audit retention settings. This means that audit results are not deleted when a system is removed from the ePolicy Orchestrator system tree. Because of this, McAfee Policy Auditor reporting queries cannot use permissions based on the system tree or a system tree subset.

If an ePolicy Orchestrator user has access to run or create report queries, the report shows audit results for all systems that have had results collected and maintained according to the policy audit retention settings, even from systems deleted from the system tree.

Contents

Policy Auditor default dashboards

McAfee Policy Auditor ships with three default dashboards, each of which has its own default monitors.

All dashboards are owned by the ePolicy Orchestrator software Global Administrators. Global Administrators must make additional dashboards active and public before other users can view them.

When you log into the ePolicy Orchestrator software, these are the visible McAfee Policy Auditor dashboards.

- PA: Compliance Summary

- PA: MS Patch Status Summary
- PA: Operations
- PA: PCI Summary

You can make other dashboards visible from the Dashboards page by clicking **Options | Select Active Dashboards**, and selecting **Available Dashboards**.

Default McAfee Policy Auditor queries

The Queries & Reports page provides a set of queries that provide high-level reports on benchmarks, checks, rules, audit results, file integrity monitoring, findings, rollup reporting, and waivers. You can run these queries or use them as starting points to create custom queries. See the ePolicy Orchestrator documentation for details on customizing and creating new queries.

The default queries are:

- **FND: Chart of Current Finding Status Types** — Pie chart of the current finding status types.
- **FND: Chart of Finding Status Grouped By Finding Identifier** — Displays a grouped summary of the Finding Status further grouped by the Finding Identifier.
- **FND: Count of Violations Grouped By Message** — Displays the count of violations grouped by the message.
- **FND: Finding Status Grouped By Finding Identifier** — Displays a grouped summary of the Finding Status that is further grouped by the Finding Identifier.
- **FND: Findings By Status and Message** — Displays the current findings grouped by their status and the finding message.
- **FND: Findings Violations** — Displays finding identifier, system, and finding messages for all findings violations.
- **FND: Grouped Summary of Finding Status for Systems** — Displays a grouped summary of a system showing the counts of finding status.
- **PA: Agent Events** — Displays a list of threat events received from the PA Agent.
- **PA: Agent Events Grouped by Event Type** — Displays a list of events reported by PA agent grouped by the event type.
- **PA: Benchmark Checks** — Displays a bar chart count of checks included in all activated benchmarks, grouped by benchmark.
- **PA: Benchmark Results - Pass/Fail/Unknown** — Pie chart of benchmark results categorized as pass/fail/unknown.
- **PA: Benchmark Rules** — Displays a count of rules included in all activated benchmarks, grouped by benchmark.
- **PA: Check Catalog List** — List of OVAL checks in the check catalog.
- **PA: Check Catalog Usage List** — List of OVAL checks used in benchmarks, including the rule and benchmark associations.
- **PA: Check Result Findings** — Pie chart of findings for current check results.
- **PA: Checks Across Benchmarks** — Displays a list of checks along with a count of their usage in activated benchmarks.
- **PA: File Entitlement** — Displays File Entitlement information for each file monitored for entitlement changes.
- **PA: File Integrity - All Events** — Displays a count of the File Integrity Events grouped by the baseline date.

- **PA: File Integrity Event Counts** — Displays a chart of File Integrity events grouped by event type.
- **PA: File Integrity Events By System/Baseline Date** — Displays a count of the File Integrity exceptions encountered after a baseline reset, grouped by system and baseline date.
- **PA: File Integrity Events By System/Event Type** — Displays a list of counts of the File Integrity Events grouped by system.
- **PA: Group Results By Benchmark Group** — Bar chart of results for groups in the benchmark. Counts are rolled up from child group to parent group.
- **PA: Group Rule Results By Benchmark Group** — Displays rule results grouped by the benchmark group.
- **PA: Group Rule Results By Rule Result** — Displays rule results for a benchmark group. The report is grouped on the rule result.
- **PA: Index Statistic List** — Displays a list of information about the indexes in the ePO database. Values are updated when the PA: Get Index and Space Statistics server task is run.
- **PA: Maintenance - Beginning Index Fragmentation Compared to 30%** — Display details on index fragmentation gathered during index maintenance. Values are updated when the PA: Maintain Database server task is run.
- **PA: Maintenance - Index Detail** — Displays information related to database index maintenance. Values are updated when the PA: Maintain Database server task is run.
- **PA: MS SLA Non-Compliant Systems Grouped By Patch and Tag** — Displays the non-compliant systems grouped by patch and tag.
- **PA: MS SLA Non-Compliant Systems Grouped By Tag and Patch** — Displays the non-compliant systems grouped by the tag and patch.
- **PA: Patches Audit** — Pie chart of benchmark results categorized as pass/fail/unknown.
- **PA: STIG Audit - Pass/Fail/Unknown** — Pie chart of benchmark results categorized as pass/fail/unknown.
- **PA: Systems by Audit** — Displays the systems assigned to an audit.
- **PA: Trend - Rollup of Systems Reporting Failed Benchmarks Status** — Displays the trend of failed benchmark audits over time, grouped by rollup server.
- **PA: Trend Of Benchmarks Reporting As Failed** — Displays the trend of benchmarks that failed during the audit process.
- **PA: Trend Of Checks Reporting As False** — Displays the trend of checks that reported as false during the audit process.
- **PA: Trend Of File Integrity Events** — Displays the trend of file integrity events received from managed systems.
- **PA: Trend Of Rules Reporting As Failed** — Displays the trend of rules that failed during the audit process.
- **PA: Unprocessed Audit Results By System** — Pie chart of unprocessed audit results grouped by system.
- **PA: Unprocessed Finding Results** — List of unprocessed finding results.
- **PA: Unprocessed Finding Results By System** — Pie chart unprocessed finding results grouped by system.

PA: Compliance Summary dashboard

The Compliance Summary dashboard provides a high-level overview of audit results with links and drill down access to detailed information.

PA: Compliance Summary dashboard

The monitors included in this dashboard are:

- **PA: Benchmark Results - Pass/Fail/Unknown** — Displays a pie chart, grouped by benchmark results and classified by status.
- **PA: Benchmark Results - Failed by Scoring Category** — Displays a pie chart grouped by scoring category.
- **PA: Rule Results By Benchmark Group** — Displays a grouped bar chart with each bar representing the number of benchmark results. The benchmark results are categorized by benchmark group.
- **PA: Benchmark Results - Fail/Unknown by L1 Group** — Displays a grouped bar chart of benchmark results, with each bar representing the number of benchmark results. The chart is categorized by first-level System Tree group where the system status is failed or unknown.
- **PA: Waivers In Effect** — Displays a list of waivers currently in effect, grouped by first-level System Tree group and classified by type of waiver.
- **PA: Errors by Rule** — Displays rules from audits that fail with a result of error.

PA: MS Patch Status Summary dashboard

The MS Patch Status Summary dashboard is a set of monitors providing a high-level overview or Microsoft patches with links and drill down access to detailed information.

PA: MS Patch Status Summary dashboard

The monitors included in this dashboard are:

- **PA: Status for MS Patch Benchmarks** — Displays a bar chart representing the deployment of all Microsoft patches, classified by status:
- **PA: MS Critical Patch Status** — Displays a pie chart representing the deployment of all critical Microsoft patches
- **PA: MS Unpatched Systems Grouped by MS Patch** — Displays the unpatched checks grouped by check ID.
- **PA: MS Patch Status Grouped by Tag** — Displays a bar chart of patch status grouped by tag.
- **PA: MS Patch Status Grouped By Severity** — Displays the patch status of Microsoft patches grouped by the vendor-assigned severity.
- **PA: Trend of Unpatched Critical MS Patches** — Displays the deployment status of all critical unpatched Microsoft patches by month. The count displayed for each month is the number of critical patches that are not patched.

PA: Operations

The Operations dashboard is a set of monitors providing a high-level overview of information about the database, unprocessed audit results, unprocessed findings results and agent events.

PA: Operations dashboard

The monitors included in this dashboard are:

- **PA: Unprocessed Audits Results by Audit** — Displays unprocessed audit results grouped by audit.
- **PA: Unprocessed Finding Results by Audit** — Displays unprocessed finding results grouped by audit.
- **PA: Agent Events Grouped by Event Type** — Displays events reported by McAfee Policy Auditor agent plug-in grouped by the event type.
- **PA: Table Space Usage** — Displays the space used by each table in the ePolicy Orchestrator database. Values are updated when the PA: Get Index and Space Statistics server task is run.
- **PA: Maintenance - Ending Index Fragmentation Compared to 30%** — Display details on index fragmentation gathered after index maintenance. Values are updated when the PA: Maintain Database server task is run.
- **PA: Last Reported Index Fragmentation Level Compared to 30%** — Displays the latest index fragmentation information gathered compared to 30%. Values are updated when the PA: Get Index and Space Statistics server task is run.

PA: PCI Summary

The Payment Card Industry (PCI) dashboard provides a high-level overview of audit results with links and drill down access to detailed information.

PA: Compliance Summary dashboard

Some reports are grouped by PCI aggregation names. These are the PCI aggregation names:

- Requirement 1: Install and maintain a firewall configuration.
- PCI Failed Systems Grouped By Aggregation.
- Requirement 3: Protect stored data .
- Requirement 4: Encrypt transmission of data across public networks.
- Requirement 5.1: Anti-virus software installed
- Requirement 5.1: Anti-virus software up-to-date
- Requirement 7: Restrict access to data
- Requirement 8: Assign a unique ID to each computer user
- Requirement 10: Track and monitor all access to network resources and data

The monitors included in this dashboard are:

- **PA: PCI Req 1: Install & Maintain Firewall Config** — Displays a pie chart grouped by scoring category.
- **PCI Req 2: Do Not Use Vendor Supplied Defaults** — Displays a grouped bar chart of benchmark results, with each bar representing the number of benchmark results. The chart is categorized by first-level System Tree group where the system status is failed or unknown.
- **PCI Req 4: Encrypt Transmission of Data** — Displays a pie chart, grouped by benchmark results and classified by status.
- **PCI Req 5: Use AV or App Whitelisting** — Displays rules from audits that fail with a result of error.

- **PCI Req 6.4: Automate documentation** — Displays a grouped bar chart with each bar representing the number of benchmark results. The benchmark results are categorized by benchmark group.
- **PCI Req 7: Restrict Access to Data** — Displays a list of waivers currently in effect, grouped by first-level System Tree group and classified by type of waiver.
- **PCI Req 8: Unique ID for each computer** — Displays a list of waivers currently in effect, grouped by first-level System Tree group and classified by type of waiver.
- **PCI Req 10.3, 10.5, 11.5: File Integrity Monitoring** — Displays a list of waivers currently in effect, grouped by first-level System Tree group and classified by type of waiver.
- **PCI Req 11.2 Run Vulnerability Scans** — Displays a list of waivers currently in effect, grouped by first-level System Tree group and classified by type of waiver.

Queries as dashboard monitors

Use any chart-based query as a dashboard that is refreshed at a user-configured frequency, so you can use your most useful queries on a live dashboard.

Policy Auditor agent plug-in debug tool

The Policy Auditor agent plug-in debug tool allows you to run audits, benchmarks, and checks on system and save the results, including debug information and the log file, to a ZIP file.

The debug tool has an interactive console interface for all operating systems as well as a graphical interface for Windows systems.

The graphical interface includes these buttons: Audits, Benchmarks, Checks, Run Selected Item, Save Debug Info, and Close. The details section shows information about a selected benchmark, audit or check.

Contents

Execute the agent plug-in debug tool

Run the debug tool from a command prompt on Windows systems or a command-line interpreter on non-Windows systems.

Task

1. Open a command prompt on a Windows system or a command-line interpreter on a non-Windows system.
2. Navigate to the folder containing the agent plug-in. On Windows systems, this is usually c:\Program Files (x86)\McAfee\Policy Auditor Agent.
3. Type the appropriate command to execute the program.

Command	Description
enginemain.exe -u	Opens the graphical version of the tool on Windows systems.
enginemain -n	Opens the interactive console version of the tool on all supported systems.

Display help

You can obtain online help on running the tool from the command prompt or command-line interface.

Task

1. Open a command prompt on a Windows system or a command-line interpreter on a non-Windows system.
2. Navigate to the folder containing the agent plug-in. On Windows systems, this is usually c:\Program Files (x86)\McAfee\Policy Auditor Agent.
3. Execute the tool, then type the appropriate command to display help.

Command	Description
engineMain.exe --help	Displays help for the graphical version of the tool on Windows systems.
help	Displays help for the interactive console version of the tool on all supported systems.

Run an audit

Run a audit on a system and save the results to a file.

Task

1. Execute the agent plug-in debug tool.
2. Save the debug information to a file.

Interface	Definition
Graphical	1 Click **Audits**. A list of available benchmarks on the system appears. 2 Select an audit that you wish to run and click **Run Selected Item**. 3 A Save As dialog box appears. Navigate to the desired location and click **OK** to save the results file.
Interactive	1 Enter resultFile <filename> to specify the path and name of the audit results file. Example: resultFile c:\test\results.xml 2 Enter auList. A list of audits and their ID appears. 3 Enter auRun <ID>. where <ID> is the audit ID. The audit results are saved to the results file specified in step 1.

Run a benchmark

Run a benchmark on a system and save the results to a file.

Task

1. Execute the agent plug-in debug tool.
2. Save the debug information to a file.

Interface	Definition
Graphical	1 Click **Benchmarks**. A list of available benchmarks on the system appears. 2 Select a benchmark that you wish to run and click **Run Selected Item**. 3 A Save As dialog box appears. Navigate to the desired location and click **OK** to save the results file.
Interactive	1 Enter resultFile <filename> to specify the path and name of the audit results file. Example: resultFile c:\test\results.xml 2 Enter bmList. A list of audits and their ID appears. 3 Enter bmRun <ID>. where <ID> is the audit ID. The audit results are saved to the results file specified in step 1.

Run a check

Run a check on a system and save the results to a file.

Task

1. Execute the agent plug-in debug tool.
2. Save the debug information to a file.

Interface	Definition
Graphical	1 Click **Checks**. A list of available checks on the system appears. 2 Select a check that you wish to run and click **Run Selected Item**. 3 A Save As dialog box appears. Navigate to the desired location and click **OK** to save the results file.
Interactive	1 Enter resultFile <filename> to specify the path and name of the audit results file. Example: resultFile c:\test\results.xml

Interface	Definition
	2 Enter ovList. A list of checks and their ID appears. **3** Enter ovRun <checkname>. where <checkname> is the name of the check. The audit results are saved to the results file specified in step 1.

Save debug information

You can save debug information, including the log file and database, to a ZIP file on the system.

Task

1. Execute the agent plug-in debug tool and perform an action, such as run an audit.
2. Save the debug information to a file.

Interface	Definition
Graphical	**1** Click **Save Debug info**. **2** In the dialog box, type a filename and location to save the ZIP file, then click **OK**.
Interactive	Enter saveDebug. The file is saved in the agent plug-in folder.

Appendix A: Implementing the Security Content Automation Protocol

McAfee Policy Auditor version 6.0 uses the Security Content Automation Protocol (SCAP) version 1.1. Security content conforming to the SCAP standard can be used by any product supporting the standard and the results can be shared between these products.

SCAP is a collection of six open standards developed jointly by various United States government organizations and the private sector. McAfee Policy Auditor uses the Security Content Automation Protocol (SCAP) to perform automated audits, including policy compliance evaluations such as the Federal Information Security Management Act (FISMA).

Contents

Statement of FDCC compliance

McAfee asserts that McAfee Policy Auditor version 6.0 does not alter or conflict with the Federal Desktop Core Configuration (FDCC) settings on Microsoft Windows XP and Vista systems.

These ports are used by McAfee Policy Auditor version 6.0.

Setting	Port	Can be edited
Agent-to-server communication	80	No
Agent wake-up communication	8081	Yes
Agent broadcast communication	8082	Yes
Console-to-application server communication	8443	Only during installation
Sensor-to-server communication	8444	Only during installation
Security threats communication	8801	Only during installation
SQL server TCP	1443	Only during installation

Statement of SCAP implementation

The Security Content Automation Protocol (SCAP) is a collection of six open standards developed jointly by various United States government organizations and the private sector. Security content conforming to the SCAP standard can be used by any product that supports the standard and the results can be shared among these products.

McAfee Policy Auditor allows users to import and export benchmarks and checks that use SCAP. Users can tailor or edit benchmarks within the McAfee Benchmark Editor interface and activate them for use in audits. Benchmarks determine whether a system complies with the benchmark rules. Benchmarks also return results that can be converted to a human-readable format.

Benchmarks and checks incorporate the following reference protocols to ensure that all rules are processed accurately and appropriately, and that the results appear properly in reports and export files:

- Common Vulnerabilities and Exposures (CVE)
- Common Configuration Enumeration (CCE)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)
- eXtensible Configuration Checklist Description Format (XCCDF)
- Open Vulnerability and Assessment Language (OVAL)

McAfee Policy Auditor version 6.0 is compliant with SCAP 1.1 and provides the ability to detect and assess thousands of systems from a McAfee Policy Auditor server. This standardization allows regulatory authorities and security administrators to construct definitive security guidance and to compare results reliably and repeatedly.

McAfee Policy Auditor is designed exclusively around SCAP and manages all aspects of analyzing systems for compliance. It uses XCCDF and OVAL to determine what items to check and how to check them. It uses the CPE, CCE, CVSS, and CVE reference protocols to ensure that all rules are accurately and appropriately evaluated during system audits. The SCAP standard references are visible in the interface, reports, and export files.

Statement of CVE implementation

McAfee Policy Auditor version 6.0 fully implements and supports the Common Vulnerabilities and Exposures (CVE) standard vulnerability dictionary. CVE provides unique, standardized identifiers for security vulnerabilities. CVE address vulnerability and exposure issues, not compliance items.

McAfee Policy Auditor implements and supports CVE enumeration, which provides standardized references to known vulnerabilities. CVE uses a named list of information security weaknesses, providing standardized identifiers to facilitate a universal naming convention. Each CVE identifier consists of:

- A CVE identifier number, such as CVE-2008-0042.
- An indication of whether the CVE has a status of "entry" or "candidate."
- A description of the vulnerability.
- A list of any references, such as advisories or OVAL identification.

McAfee Policy Auditor patch and vulnerability definitions are updated periodically when new content is available. The audit results can be viewed from the Audits, Reports, or Dashboard user interfaces.

CVE information is accessible from the Checks interface, which displays details of Common Vulnerabilities. Users have the ability to view even more detailed CVE information from the Check Details page, which displays the Source, ID, and URL. For example, the URL http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2122 refers the user to the Mitre site to view details about CVE-2005-2122. The security content provided by McAfee refers to CVE identifiers when addressing vulnerabilities and whether a vendor's patch has been applied to address the vulnerability.

Previous versions of McAfee Policy Auditor have been certified by Mitre as CVE-Compatible.

Statement of CCE implementation

CCE provides a standard system for identifying and referencing system configuration settings. CCE identifies the configuration itself, not the means by which that configuration was reached. CCE encourages interoperability, improves the correlation of test results, and simplifies gathering metrics.

McAfee Policy Auditor includes CCE references in the checks content. The Checks tab lists all the checks available to users. Clicking on a check with CCE content lists CCE references that identify the CCE system configuration settings.

McAfee Policy Auditor version 6.0 incorporates and supports version 5.0 of the Common Configuration Enumeration (CCE) standard. Previous versions of McAfee Policy Auditor have been certified by Mitre as CCE-Compatible.

Statement of CPE implementation

McAfee Policy Auditor version 6.0 implements version 2.1 of the Common Platform Enumeration (CPE) standard. CPE provides a standard reference and notation method for information technology systems, platforms, and packages.

McAfee Policy Auditor contains the CPE data dictionary in the database with some of it in aggregated format to promote ease of use. Information from this dictionary drives various aspects of the McAfee Policy Auditor interface. McAfee Policy Auditor associates OVAL definitions with CPE Names and allows users to specify CPE names at the benchmark, group, profile, or rule level. McAfee Policy Auditor users can create audits with SCAP content that cover a number of common operating systems and platforms.

When CPE platforms are specified, McAfee Policy Auditor uses this information to determine whether it should evaluate compliance with a rule or group of rules. For example, an audit can cover both Windows XP and Windows Vista operating systems but not the Windows 2000 operating system. CPE allows McAfee Policy Auditor to use the correct content on the correct systems.

Previous versions of McAfee Policy Auditor have been certified by Mitre as CPE-Compatible.

Statement of CVSS implementation

McAfee Policy Auditor version 6.0 incorporates version 2.0 of the Common Vulnerability Scoring System (CVSS). CVSS is a standardized open framework for measuring the impact of vulnerabilities.

Each CVE includes an associated CVSS vector to determine the relative severity of vulnerabilities. CVSS is built on a quantitative model that ensures repeatable measurements on systems, valid comparisons between systems, and that allows users to view the underlying vulnerability characteristics. Using CVSS scores help an organization to determine and prioritize responses to detected vulnerabilities.

McAfee Policy Auditor supports all four standard SCAP scoring models:

- Flat
- Unweighted
- Absolute
- Default

The default setting for McAfee Policy Auditor is a flat unweighted scoring model normalized to a maximum possible score of 100. The scoring model can be changed for comparison purposes.

Previous versions of McAfee Policy Auditor have been certified by Mitre as CVSS-Compatible.

Statement of XCCDF implementation

The eXtensible Configuration Checklist Description Format (XCCDF) is an XML specification language that supports the exchange of information, generation of results, tailoring, automated compliance testing, and compliance scoring. It also provides a data model and format for storing results of benchmark compliance testing.

XCCDF provides a uniform standard for the expression of benchmarks and other configuration guidance to encourage good security practices. McAfee Policy Auditor uses benchmarks from McAfee or third-party sources to construct audits. Users can select the benchmark profile, if any, to use for the audit. After a system is audited, the audit results are returned to McAfee Policy Auditor, which analyzes and reports on the configuration and vulnerability data. The user can specify how long audit data is retained so that they or auditors can review any changes in the state of a system over time.

McAfee Policy Auditor version 6.0 implements version 1.1.4 of XCCDF. Previous versions of McAfee Policy Auditor have been certified by Mitre as XCCDF-Compatible.

Statement of OVAL implementation

The Open Vulnerability and Assessment Language (OVAL) describes the ideal configuration of systems, compares systems to the ideal configuration, and reports the test results. It provides a structured model for network and system administrators to detect vulnerabilities and configuration issues on systems.

McAfee Benchmark Editor uses the Checks interface to import and export OVAL definitions and other formats supported by XCCDF. These checks can be filtered based on OVAL IDs, platforms, or any other criteria set by the user. The Check Details interface displays a hyperlink to specific OVAL IDs, which will display OVAL in XML format.

When a system is audited, the OVAL content is processed according to the information in the XCCDF benchmarks contained in the audit. The OVAL content captures the state of the system at the particular point in time that the audit is run. The results are returned to McAfee Policy Auditor for analysis and reporting. The user specifies how long audit data is to be retained so that they or auditors can review any changes in the state of a system over time.

McAfee Policy Auditor version 6.0 provides fully integrated support for OVAL versions 5.7, 5.8, and 5.9. Previous versions of McAfee Policy Auditor have been certified by Mitre as OVAL-Compatible.

Appendix B: Common Criteria requirements

ePolicy Orchestrator software has functional modifications that meet specific Common Criteria requirements.

This information is intended for use by government agencies that are required to use only National Information Assurance Partnership (NIAP) Common Criteria validated security products. It describes functional modifications that meet specific Common Criteria requirements, and provides advice on best practices for satisfying those requirements.

Server access

Physical access to the server must be restricted to authorized personnel that have been adequately trained to manage the system.

The server must be located in a physically secure facility with access limited to authorized personnel.

Functionality on multiple platforms

The combination of ePolicy Orchestrator software and McAfee Policy Auditor software functions identically on all platforms where they operate.

Encryption

All packages created and distributed by McAfee are signed with a key pair using the DSA (Digital Signature Algorithm) signature verification system, and are encrypted using 168-bit 3DES encryption. A key is used to encrypt or decrypt sensitive data.

The ePolicy Orchestrator software repository list (SiteList.xml) file contains the names of all the repositories you are managing. The repository list includes the location and encrypted network credentials that managed systems use to select the repository and retrieve updates. The server sends the repository list to the agent during agent-server communication.

The Security Keys page in the ePolicy Orchestrator software allows you to manage encryption for repositories and for agent-server communications.

Applications running under the ePolicy Orchestrator software environment use a Secure Socket Layer (SSL) sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks.

HTTPS and SSL support the use of X.509 digital certificates from the server so that a user can authenticate the sender.

Passwords

When a new ePolicy Orchestrator software user is created, the Add New User interface allows for use of NT authentication, which has previously been set at the network level, or a new ePolicy Orchestrator software authentication credential can be created.

Administrators who must adhere to the requirements of the National Information Assurance Partnership (NIAP) Common Criteria Validation Scheme (CCEVS) are directed to assign passwords employing ePolicy Orchestrator software authentication only. McAfee recommends that the network IT administrator assign passwords that meet the following requirements:

- Must be at least 10 characters in length.
- Must contain at least three of the following four character groups:
  - English uppercase characters (A-Z).
  - English lowercase characters (a-z).
  - Numerals (0-9).
  - Non-alphanumeric characters, such as !, $, #, %.

User IDs and passwords should be unique. No two users should have the same password. In addition, the User ID used to access ePolicy Orchestrator software should be different from any other User ID required for related ePolicy Orchestrator software functionality such as SQL administration or creation of distributed repositories.

Administrators must ensure that all user names and passwords are protected by the users in a manner which is consistent with IT security.

Intrusion prevention system

McAfee Host Intrusion Prevention System software is a preemptive approach to host and network security used to identify and quickly respond to potential threats. McAfee Host Intrusion Prevention System monitors individual host and network traffic. However, because an attacker might carry out an attack immediately after gaining access, McAfee Host Intrusion Prevention System can also take immediate action as preset by the network administrator.

Timestamp

ePolicy Orchestrator software uses either a *datetime* or *smalldatetime* data type, as appropriate, to record the events and triggers to automatically update the timestamp when any modification takes place. Many tables have a *datetime* or *smalldatetime* data type to indicate when a row was created, and are linked to other tables to preserve the date and time of all modifications.

Email alarm notifications of storage space exhaustion

The ePolicy Orchestrator software notification feature transmits alerts to designated email recipients. The administrator must set up four Notifications that require configuration in order to meet the “alarm” requirements of FAU_STG.4.1 and IDS_STG.2.1

- Notification that storage space for new records in the ePOAuditEvent table in the SQL Server database is exhausted.
- Purging of the oldest 20% of the records in the ePOAuditEvent table completed successfully.
- Purging of the oldest 20% of the records in the ePOAuditEvent table failed.
- Notification that storage space for new records in the ENT_IPSEvent table in the SQL Server database is exhausted. When this notification is received, the administrator should purge the database.

The appropriate version of the *ePolicy Orchestrator software Product Guide* provides information about purging and archiving the database.

Index