

McAfee Security 1.0 User Guide

COPYRIGHT

Copyright © 2009 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFFEE SECURITYALLIANCE EXCHANGE), MCAFFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE INFORMATION

License Agreement

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

License Attributions

Refer to the product Release Notes.

Contents

- Introducing McAfee Security 1.0..... 5**
 - How McAfee Security works..... 5
 - New features in this release..... 5

- Installing and managing McAfee Security on standalone computers..... 7**
 - Prerequisites..... 7
 - Methods of installation..... 7
 - Standard installation..... 8
 - Command-line (silent) installation..... 8
 - Testing the Anti-malware feature..... 8
 - Uninstalling McAfee Security..... 9

- Integrating McAfee Security with McAfee ePolicy Orchestrator 4.0..... 10**
 - Prerequisites..... 10
 - Deploying McAfee Security using ePolicy Orchestrator 4.0..... 10
 - Checking-in the McAfee Agent and McAfee Security package to ePolicy Orchestrator 4.0..... 11
 - Installing McAfee Agent on client computers..... 11
 - Installing McAfee Security extensions..... 11
 - Installing McAfee Security on client computers..... 12
 - Setting policies using ePolicy Orchestrator 4.0..... 12
 - Creating policies..... 12
 - Enforcing policies..... 12
 - Scheduling tasks using ePolicy Orchestrator 4.0..... 13
 - On-demand scan task..... 13
 - Removing McAfee Security using ePolicy Orchestrator 4.0..... 13
 - Removing McAfee Security from the client computers..... 14
 - Removing McAfee Security extensions from the ePolicy Orchestrator server..... 14

- Integrating McAfee Security with McAfee ePolicy Orchestrator 4.5..... 15**
 - Deploying McAfee Security using ePolicy Orchestrator 4.5..... 15
 - Checking-in the McAfee Agent and McAfee Security package to ePolicy Orchestrator 4.5..... 15
 - Installing McAfee Agent on client computers..... 16
 - Installing McAfee Security extensions..... 16
 - Installing McAfee Security on client computers..... 17

Setting policies using ePolicy Orchestrator 4.5.	17
Creating policies.	17
Enforcing policies.	18
Scheduling tasks using ePolicy Orchestrator 4.5.	18
On-demand scan task.	18
Removing McAfee Security using ePolicy Orchestrator 4.5.	18
Removing McAfee Security from the client computers.	19
Removing extensions from the ePolicy Orchestrator server.	19
Launching McAfee Security Console.	20
Dashboard with the latest events.	20
History of all events.	21
Quarantining malware.	22
Default activities in McAfee Security Console.	23
Update Now.	23
Scan Now.	24
Configuring scan tasks.	24
Creating a new scan task.	24
Modifying an existing scan task.	24
Deleting a scan task.	25
Configuring McAfee Security Preferences.	26
General Preferences.	26
Configuring Anti-malware Preferences.	27
Configuring On-access Scan Preferences.	27
Configuring On-demand Scan Preferences.	29
Specifying Anti-malware Exclusions.	30
Enhanced Notification Report.	30
Update Preferences.	31
Default Preferences.	32
Help option in the menu bar.	32

Introducing McAfee Security 1.0

McAfee Security 1.0 has an enhanced graphical user interface and protects your Mac from malware.

Topics covered in this chapter are:

Contents

- ▶ [How McAfee Security works](#)
- ▶ [New features in this release](#)

How McAfee Security works

McAfee Security 1.0 scans files, folders, local or network mounted volumes, and other items for malware or potentially unwanted code and notifies you in case of malware detections. Scanning takes place every time you create or access an item. You can also schedule scans to run immediately, at a particular time, or at regular intervals.

McAfee Security integrates with your Mac OS and works in real-time to detect malware. It scans files, folders, local or network mounted volumes, and other items for potentially unwanted code and notifies you in case of malware detections. Scanning takes place every time you create or access an item. You can also schedule scans to run immediately, at a particular time, or at regular intervals.


Central to your McAfee Security software are the McAfee Security scanning engine and the malware definition files (DATs). The engine is a complex data analyzer. It identifies the type of the item being scanned and decodes the content of that object to understand what the item is. It then scans items on your Mac comparing them with all known signatures stored in the DAT files. The DAT files contain a great deal of information including thousands of different drivers; each of which contain detailed instructions on how to identify malware (based on their signatures).

New features in this release

New features of McAfee Security includes:

Core features

Option	Definition
Support for Snow Leopard	In addition to Mac OS X Tiger and Mac OS X Leopard, McAfee Security supports Mac OS X Snow Leopard 10.6 or later.

Option	Definition
McAfee menulet for easy access of McAfee Security	<p>Click the McAfee menulet  to launch McAfee Security Console, McAfee Security Preferences, and the About dialog box.</p> <p>TIP: For more information, refer to the <i>Menulet options</i> section.</p>
Enhanced dashboard	<p>McAfee Security offers an enhanced dashboard that displays the security status and the latest anti-malware events.</p> <p>TIP: For more information, refer to the <i>Dashboard</i> section.</p>
History of all events	<p>The History screen displays all anti-malware events.</p> <p>Click History on the left pane of the McAfee Security console to view all anti-malware events.</p> <p>TIP: For more information, refer to the <i>History of all events</i> section.</p>
Quarantine malware	<p>McAfee Security quarantines malware (or suspected malware-like behavior) to a location you specified while installing McAfee Security, so that the item cannot be opened or executed.</p> <p>TIP: For more information, refer to the <i>Quarantining malware</i> section.</p>
Enhanced notification mechanism	<p>You are notified of malware detections (resulting from on-access scan) in the McAfee Notification screen.</p>
ePolicy Orchestrator manageability (optional)	<p>You can deploy and manage McAfee Security across multiple client computers using McAfee ePolicy Orchestrator 4.0 or later.</p>

Additional features

Support for:

- Specifying extended set of primary and secondary actions for on-access and on-demand scans.
- Specifying regular expression based exclusions for on-access and on-demand scans separately.
- Running multiple on-demand scans immediately at the same time.
- Scheduling multiple on-demand scans to run simultaneously.
- Enhanced MER tool for collecting diagnostic data of the software.

Installing and managing McAfee Security on standalone computers

McAfee Security can be installed on standalone systems using the standard installation or command-line (silent) installation method. Topics covered in this chapter are:

Contents

- ▶ Prerequisites
- ▶ Methods of installation
- ▶ Testing the Anti-malware feature
- ▶ Uninstalling McAfee Security

Prerequisites

Hardware requirements

Option	Definition
Processor	Intel or PowerPC
RAM	1 GB or higher

Software requirements

Option	Definition
Disk space	Minimum 300 MB of free disk space (500 MB recommended)
Operating system	<ul style="list-style-type: none">• Mac OS X Snow Leopard 10.6 or later• Mac OS X Leopard 10.5 or later• Mac OS X Tiger 10.4.6 or later

Methods of installation

You can install McAfee Security using one of the following methods:

Tasks

- ▶ Standard installation
- ▶ Command-line (silent) installation

Standard installation

Standard installation includes installing McAfee Security by running the user interface installer. During standard installation, a wizard appears leading the installation process through a series of instructions you must follow.

Prerequisite: You must have administrator rights to install McAfee Security.

- 1 Download **McAfee Security for Mac-1.0-<release-type>-<build-number>.dmg** to your desktop and double-click it to mount.
- 2 Double-click **McAfee Security.mpkg**. The **Welcome to the McAfee Security Installer** screen appears.
- 3 Click **Continue** and follow the on-screen instructions to install the software.

NOTE: The installer places the McAfee Security application in **/Applications**.

Command-line (silent) installation

Command-line installation involves installing McAfee Security locally on a computer without the need for user intervention.

- 1 Download **McAfee Security for Mac-1.0-<release-type>-<build-number>.dmg** to your desktop.
- 2 Locate the **McAfee Security.mpkg** file in the DMG file downloaded from the McAfee website, then save it to a temporary location.
- 3 Open the Terminal window and change the working directory to the one where you saved the **McAfee Security.mpkg** file.
- 4 Type the following command and press **return**:
`sudo installer -pkg McAfeeSecurity.mpkg -target /`
- 5 Type the administrator password when prompted and press **return**. A message appears when the installation is complete.

Menulet options

After McAfee Security is installed, you can click the McAfee menulet  to launch:

- **McAfee Security Console** — To view the five latest product events, security status of your Mac, status of on-accessing scanning, instance of the last anti-malware update, history of all product events, quarantined malware, and configure manual updates/scans.
- **McAfee Security Preferences** — To configure the general, anti-malware, and update preferences (settings).
- **About** dialog box — To get the following information:
 - Version (and build) information of McAfee Security.
 - Anti-malware information that includes the version (and build) information, Engine version, DAT version, and the DAT creation date.

Testing the Anti-malware feature

You can test McAfee Security by using the European Institute of Computer Anti-Virus Research (EICAR) standard anti-virus test file. This file is a combined effort by anti-virus vendors

throughout the world to implement one standard by which customers can verify their anti-virus software.

- 1 Go to the EICAR.ORG website <http://www.eicar.org> and download the anti-virus test file **Eicar.com**.
- 2 Run the on-demand scanner on the downloaded ZIP file. McAfee Security will report finding the EICAR test file.

Uninstalling McAfee Security

You can uninstall McAfee Security from **Finder** or through command-line.

Prerequisites: You must have administrator rights to uninstall McAfee Security.

Uninstalling McAfee Security from Finder

- 1 Launch **Finder**, go to **Applications**, then double-click **McAfeeSecurityUninstaller**.
- 2 Type the administrator password when prompted and press **return**.

Uninstalling McAfee Security through command-line

- 1 In the Terminal window, type the following command and press **return**.
`/usr/local/McAfee/uninstallMSC`
- 2 When prompted, type your password and press **return**.
When the uninstallation process completes, the Terminal displays a message stating that McAfee Security is uninstalled from your Mac.

Integrating McAfee Security with McAfee ePolicy Orchestrator 4.0

This chapter describes how to configure McAfee Security using McAfee ePolicy Orchestrator management software version 4.0. To use this chapter effectively, you need to be familiar with ePolicy Orchestrator 4.0.

McAfee ePolicy Orchestrator 4.0 provides a scalable platform for centralized policy management and enforcement on your McAfee security products and systems on which they reside. It also provides comprehensive reporting and product deployment capabilities; all through a single point of control.

NOTE: This document does not provide detailed information about installing or using ePolicy Orchestrator software. See the McAfee ePolicy Orchestrator 4.0 product documentation for more information.

Topics covered in this chapter are:

- ▶ [Prerequisites](#)
- ▶ [Deploying McAfee Security using ePolicy Orchestrator 4.0](#)
- ▶ [Scheduling tasks using ePolicy Orchestrator 4.0](#)
- ▶ [Removing McAfee Security using ePolicy Orchestrator 4.0](#)

Prerequisites

Before using the ePolicy Orchestrator software to manage McAfee Security, install the McAfee Agent 4.0 on the client computers.

McAfee Agent is a component of ePolicy Orchestrator that must be installed on each client computer on the network. It collects and sends information between the ePolicy Orchestrator server and its client computers, and manages McAfee Security installations across the network.

Deploying McAfee Security using ePolicy Orchestrator 4.0

Topics covered in this section are:

Content

- ▶ [Installing McAfee Agent on client computers](#)
- ▶ [Installing McAfee Security extensions](#)
- ▶ [Installing McAfee Security on client computers](#)

Checking-in the McAfee Agent and McAfee Security package to ePolicy Orchestrator 4.0

You can check-in the McAfee Agent package and McAfee Security package from the **Repository** page. Repository is the central location for all McAfee updates residing on the ePolicy Orchestrator server. It retrieves user-specified updates from the McAfee site or user-defined source sites.

- 1 Copy the **MSA-MAC 4.0.0 Build <build number> Package #4 (ENU-LICENSED-RELEASE-PATCH1).zip** and **McAfee Security for Mac-1.0-ePO-<build number>.zip** files to a temporary location of your ePolicy Orchestrator computer.
- 2 Log on to the ePolicy Orchestrator server as an administrator.
- 3 Click **Software | Check in Package**. The **Check In Package** page appears.
- 4 Select the **Package type** as **Product or Update (.ZIP)**. Browse in **File path** to locate and check-in the **MSA-MAC 4.0.0 Build <build number> Package #4 (ENU-LICENSED-RELEASE-PATCH1).zip** file.
- 5 Click **Next**. The **Package Options** page appears with the package information.
- 6 Click **Save**.

NOTE: Repeat the same steps and in step 4, check-in the McAfee Security package **McAfee Security for Mac-1.0-ePO-<build number>.zip**.

Installing McAfee Agent on client computers

After checking-in the McAfee Agent package to the ePolicy Orchestrator server 4.0, you should manually install McAfee Agent 4.0 on the client computers.

- 1 Copy install.sh file from the following location to the client computer(s):
<ePO install directory>\DB\Software\Current\EPOAGENT3700MACX\Install\0409
- 2 Type **sh install.sh -i** in the Terminal window and press **return**.
To upgrade the agent, you can type **sh install.sh -u** in the Terminal window and press **return**.

Important: You must log on as a root user to execute the **sh install.sh** command. The **sh install.sh** file is created automatically after you check-in the Agent package in to the ePolicy Orchestrator server.

Installing McAfee Security extensions

- 1 Copy the **McAfee_Security_for_Mac_Anti_malware_AVAS.zip** to a temporary location of your ePolicy Orchestrator computer.
- 2 Log on to the ePolicy Orchestrator server as an administrator.
- 3 Click **Configuration | Extensions | Install Extension**. The **Install Extension** dialog box appears.
- 4 Click **Browse** to install the anti-virus extension file **McAfee_Security_for_Mac_Anti_malware_AVAS.zip**, then click **OK**.
- 5 Click **OK**.

NOTE: Repeat the same steps to install the following extension:

- **McAfee_Security_for_Mac_Reports.zip** (Reports extension)

Installing McAfee Security on client computers

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Systems**, select the required system(s), click **Client Tasks** tab, then **New Task**. The **Client Task Builder** page appears.
- 3 In **Description**, type a **Name**, **Notes** (optional), select the **Type** as **Product Deployment (McAfee Agent)**, then click **Next**.
- 4 In **Configuration**, select **Mac** as **Target Platforms**, **McAfee Security for Mac 1.0** as **Products and components**, and **Install** as **Action**, then click **Next**.
- 5 Schedule the task to run immediately or as required, then click **Next** to view a summary of the task.
- 6 Click **Save**, then send an agent wake-up call.

Setting policies using ePolicy Orchestrator 4.0

You can create, edit, delete and enforce policies to a specific group/system(s) in the **System Tree**.

- ▶ [Creating policies](#)
- ▶ [Enforcing policies](#)

Creating policies

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Systems** | **System Tree** and choose a desired group/system(s).
- 3 Click **Policies**, select the following options from the **Product** drop-down list.
 - **McAfee Security for Mac 9.0.0:Anti-malware**A list of policies managed by the chosen point product appears in the lower pane.
- 4 Locate a policy category, then click **Edit Assignment**. The **Policy assignment for My Organization** page appears.
- 5 Click **New policy**. The **Create a new policy** dialog box appears. Choose **McAfee Default** or **My Default** as required.

NOTE: The **McAfee Default** policy is read-only and cannot be edited, renamed, or deleted.
- 6 Type a **New policy name**, then click **OK**.
- 7 Configure the anti-malware preferences as required, then click **Save**.
- 8 Click **Save** again.

Enforcing policies

You can enforce a policy to multiple managed nodes within a group.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Systems**. In **System Tree**, select the required system(s).
- 3 Click **Modify Policies on a Single System**.

- 4 Select the required **Product**, click the policy link, and configure the appropriate policy as required.
- 5 Click **Save**, then **Close**.
- 6 Send an agent wake-up call.

NOTE: In step 2, if you select group(s):

- 1 Click the **Policies** tab, select the required **Product**, click the policy link, and configure the appropriate policy as required.
- 2 Click **Save**.
- 3 Send an agent wake-up call.

Scheduling tasks using ePolicy Orchestrator 4.0

ePolicy Orchestrator allows you to create, schedule and maintain client tasks that run on the managed systems. You can define client tasks for the entire System Tree, a specific group, or an individual system.

On-demand scan task

You can schedule multiple on-demand scan tasks to run immediately, at specific times, or at regularly-scheduled intervals across managed nodes.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Systems | System Tree | Client Tasks**.
- 3 Select the desired group in the **System Tree** for which you want to create the on-demand scan task.
- 4 Click **New Task**. The **Client Task Builder** page appears.
- 5 Under **Description**, type a **Name** and **Notes** (optional) for the on-demand scan task.
- 6 Select **On Demand Scan (McAfee Security for Mac 9.0.0:Anti-malware)** as the **Type** of the task and click **Next**.
- 7 In **Configuration**, add the file(s) to be scanned.
- 8 Click **Next** and schedule the task as desired
- 9 Click **Next** to view the summary of the on-demand scan task.
- 10 Click **Save**, then send an agent wake-up call.

Removing McAfee Security using ePolicy Orchestrator 4.0

This section provides instructions to uninstall McAfee Security from the client computers and remove the extensions from the ePolicy Orchestrator server.

- ▶ [Removing McAfee Security from the client computers](#)
- ▶ [Removing McAfee Security extensions from the ePolicy Orchestrator server](#)

Removing McAfee Security from the client computers

- 1 Click **Systems**, select the required system(s), click **Client Tasks** tab, then **New Task**. The **Client Task Builder** page appears.
- 2 In **Description**, type a **Name**, **Notes** (optional), select the **Type** as **Product Deployment (McAfee Agent)**, then click **Next**.
- 3 In **Configuration**, select **Mac** as **Target Platforms**, **McAfee Security for Mac 1.0** as **Products and components**, **Install** as **Remove** and an appropriate **Language**, then click **Next**.
- 4 Schedule the task to run immediately or as required, then click **Next** to view a summary of the task.
- 5 Click **Save**, then send an agent wake-up call.

Removing McAfee Security extensions from the ePolicy Orchestrator server

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Configuration | Extensions**.
- 3 Select the following extension files (one at a time), then click **Remove**.
 - **McAfee Security for Mac 9.0.0:Anti-malware**
 - **McAfee Security for Mac Reports**
- 4 Select the option **Force removal, bypassing any checks or errors**.

NOTE: This step is not mandatory, but recommended.
- 5 Click **OK**.

Integrating McAfee Security with McAfee ePolicy Orchestrator 4.5

This chapter describes how to configure McAfee Security using McAfee ePolicy Orchestrator management software version 4.5. To use this chapter effectively, you need to be familiar with ePolicy Orchestrator 4.5.

McAfee ePolicy Orchestrator 4.5 provides a scalable platform for centralized policy management and enforcement on your McAfee security products and systems on which they reside. It also provides comprehensive reporting and product deployment capabilities; all through a single point of control.

NOTE: This document does not provide detailed information about installing or using ePolicy Orchestrator software. See the McAfee ePolicy Orchestrator 4.5 product documentation for more information.

Topics covered in this chapter are:

Contents

- ▶ [Deploying McAfee Security using ePolicy Orchestrator 4.5](#)
- ▶ [Setting policies using ePolicy Orchestrator 4.5](#)
- ▶ [Scheduling tasks using ePolicy Orchestrator 4.5](#)
- ▶ [Removing McAfee Security using ePolicy Orchestrator 4.5](#)

Deploying McAfee Security using ePolicy Orchestrator 4.5

Topics covered in this section are:

Contents

- ▶ [Installing McAfee Agent on client computers](#)
- ▶ [Installing McAfee Security extensions](#)
- ▶ [Installing McAfee Security on client computers](#)

Checking-in the McAfee Agent and McAfee Security package to ePolicy Orchestrator 4.5

You can check-in the Agent package and McAfee Security package from the **Packages in Master Repository** page.

- 1 Copy the **MSA-MAC 4.0.0 Build <build number> Package #4 (ENU-LICENSED-RELEASE-PATCH1).zip** and **McAfee Security for Mac-1.0-ePO-<build number>.zip** files (from the **ePO Server Components** folder) to a temporary location of your ePolicy Orchestrator computer.
- 2 Log on to the ePolicy Orchestrator server as an administrator.
- 3 Click **Menu | Software | Master Repository**. The **Packages in Master Repository** page appears.
- 4 Click **Actions | Check In Package**. The **Package** page appears.
- 5 Select the **Package type** as **Product or Update (.ZIP)**. Browse in **File path** to locate and check-in the **MSA-MAC 4.0.0 Build <build number> Package #4 (ENU-LICENSED-RELEASE-PATCH1).zip** file.
- 6 Click **Next**. The **Package Options** page appears with the package information.
- 7 Click **Save**.

NOTE: Repeat the same steps and check-in the McAfee Security package **McAfee Security for Mac-1.0-ePO-<build number>.zip**.

Installing McAfee Agent on client computers

After checking-in the McAfee Agent package to the ePolicy Orchestrator server 4.5, you must manually install McAfee Agent 4.0 on the client computers.

- 1 Copy **install.sh** file from the following location to the client computer.
<ePO install directory>\DB\Software\Current\EPOAGENT3700MACX\Install\0409
- 2 Type **sh install.sh -i** in the Terminal window and press **return**.
To upgrade the agent, you can type **sh install.sh -u** in the Terminal window and press **return**.

Important: You must log on as a root user to execute the **sh.install.sh** command. The **sh.install.sh** file is created automatically after you check-in the Agent package in to the ePolicy Orchestrator server.

Installing McAfee Security extensions

- 1 Copy the **McAfee_Security_for_Mac_Anti_malware_AVAS.zip** to a temporary location of your ePolicy Orchestrator computer.
- 2 Log on to the ePolicy Orchestrator server as an administrator.
- 3 Click **Menu | Software | Extensions | Install Extension**. The **Install Extension** dialog box appears.
- 4 Click **Browse** to install the anti-virus extension file **McAfee_Security_for_Mac_Anti_malware_AVAS.zip**, then click **OK**.
- 5 Click **OK**.

NOTE: Repeat the same steps to install the following extension:

- **McAfee_Security_for_Mac_Reports.zip** (Report extension)

Installing McAfee Security on client computers

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the systems from on you want to install McAfee Security.
- 3 Click **Client Tasks | Actions | New Task**. The **Client Task Builder** page appears.
- 4 In **Description**, type a **Name**, **Notes** (optional), select the **Type** as **Product Deployment**, then click **Next**.
- 5 In **Configuration**, select **Mac** as **Target Platforms**, **McAfee Security for Mac 1.0** as **Products and components**, **Install** as **Action** and the appropriate **Language**, then click **Next**.
- 6 Schedule the task to run immediately or as required, then click **Next** to view a summary of the task.
- 7 Click **Save**, then send an agent wake-up call.

Setting policies using ePolicy Orchestrator 4.5

The ePolicy Orchestrator console allows you to enforce policies across multiple Macs. These policies override configurations set on individual Macs. For information regarding policies and how they are enforced, see the McAfee ePolicy Orchestrator 4.5 Product Guide.

After you have modified the appropriate policies and saved the changes for the intended computer or group of computers, you are ready to deploy new settings via the McAfee Agent. You can create, edit, delete, or assign a policy to a specific group/system.

- ▶ [Creating policies](#)
- ▶ [Enforcing policies](#)

Creating policies

You can create, edit, delete, or assign a policy to a specific group in the System Tree.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree | Assigned Policies**.
- 3 Select the following options (one at a time) from the **Product** drop-down list:
 - **McAfee Security for Mac 9.0.0:Anti-malware**A list of policies managed by the chosen point product appears in the lower pane.
- 4 Locate the required policy, then click **Edit Assignment**.
- 5 Click **New policy** or **Edit policy** as required. The **Create a new policy** dialog box appears. Choose **McAfee Default** or **My Default** as required.

NOTE: The **McAfee Default** policy is read-only and cannot be edited, renamed, or deleted.

- 6 Type a **New policy name**, then click **OK**.
- 7 Configure the anti-malware preferences as required (based on the option you selected in step 3), then click **Save**.
- 8 Click **Save** again.

Enforcing policies

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree** select the required system(s).
- 3 Click **Actions | Agent | Modify Policies on a Single System**.
- 4 Select the required **Product**, click the policy link, and configure the appropriate policy as required.
- 5 Click **Save**, then **Close**.
- 6 Send an agent wake-up call.

NOTE: In step 2, if you select group(s):

- 1 Click the **Assigned Policies** tab, select the required **Product**, click the policy link, and configure the appropriate policy as required.
- 2 Click **Save**.
- 3 Send an agent wake-up call.

Scheduling tasks using ePolicy Orchestrator 4.5

ePolicy Orchestrator allows you to create, schedule and maintain client tasks that run on the managed systems. You can define client tasks for the entire System Tree, a specific group, or an individual system.

On-demand scan task

You can schedule multiple on-demand scan tasks to run immediately, at specific times, or at regularly-scheduled intervals across managed nodes.

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree** and select a required group or system(s).
- 3 Click **Client Task | Actions | New Task**. The **Client Task Builder** page appears.
- 4 In **Description**, type a **Name** and **Notes** (optional) for the on-demand scan task.
- 5 Select **On Demand Scan (McAfee Security for Mac 9.0.0:Anti-malware)** as the **Type** of the task and click **Next**.
- 6 In **Configuration**, add the file(s) to be scanned.
- 7 Click **Next** and schedule the task as desired
- 8 Click **Next** to view the summary of the on-demand scan task.
- 9 Click **Save**, then send an agent wake-up call.

Removing McAfee Security using ePolicy Orchestrator 4.5

This section provides instructions to uninstall McAfee Security from the client computers and remove the extensions from the ePolicy Orchestrator server.

- ▶ Removing McAfee Security from the client computers
- ▶ Removing extensions from the ePolicy Orchestrator server

Removing McAfee Security from the client computers


- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Systems | System Tree**, then select the systems from which you want to uninstall McAfee Security.
- 3 Click **Client Tasks | Actions | New Task**. The **Client Task Builder** page appears.
- 4 In **Description**, type a **Name**, **Notes** (optional), select the **Type** as **Product Deployment**, then click **Next**.
- 5 In **Configuration**, select **Mac** as **Target Platforms**, **McAfee Security for Mac 1.0** as **Products and components**, **Remove** as **Action** and the appropriate **Language**, then click **Next**.
- 6 Schedule the task to run immediately or as required, then click **Next** to view a summary of the task.
- 7 Click **Save**, then send an agent wake-up call.

Removing extensions from the ePolicy Orchestrator server

- 1 Log on to the ePolicy Orchestrator server as an administrator.
- 2 Click **Menu | Software | Extensions**.
- 3 Click **McAfee Security for Mac** on the left pane.
- 4 Click the **Remove** link of the product extensions.
- 5 Select the option **Force removal, bypassing any checks or errors**, then click **OK**.
NOTE: This step is not mandatory, but recommended.
- 6 Click **OK**.

Launching McAfee Security Console

You can launch McAfee Security Console using one of the following methods:

- Click the McAfee menulet  on your status bar, then select **McAfee Security Console**.
- Launch **Finder**, go to **Applications**, then double-click **McAfee Security**.

From the left pane of the console, you can navigate to the enhanced McAfee Security **Dashboard**, **History** screen displaying all product events, **Quarantine** screen that provides information on quarantined items, and the **Update Now** and **Scan Now** activities.

Topics covered in this chapter are:

Contents

- ▶ [Dashboard with the latest events](#)
- ▶ [History of all events](#)
- ▶ [Quarantining malware](#)
- ▶ [Default activities in McAfee Security Console](#)
- ▶ [Configuring scan tasks](#)

Dashboard with the latest events

Dashboard is the default screen that comes up when you launch McAfee Security Console. McAfee Security has an enhanced dashboard that displays:

- Five latest events related to scanning and anti-malware updates.
- Status of your Mac security and on-access scanning.
- Instance of the last anti-malware update.

The events mainly include:

- **Anti-malware Update** — Double-clicking this event displays a dialog box that provides information on the DAT version, Engine version, and the status of the update.
- **On-access Scan** — Double-clicking this event displays a dialog box that provides information on the process that accessed the item, status of the scan (whether an item was detected or not), total number of detected items, name and location of the infected files, and the action taken when they were detected.
- **On-demand Scan** — Double-clicking this event displays a dialog box that provides information on the number of files that were and were not scanned, name and location of the infected files, and the action taken when they were detected.

Sorting events

To sort events alphabetically, click the column headers on the screen. Alternatively, you can click **History** on the **McAfee Security** menu bar, select **Arrange By**, then select **Event Type**, or **Date & Time** as required.

Removing events

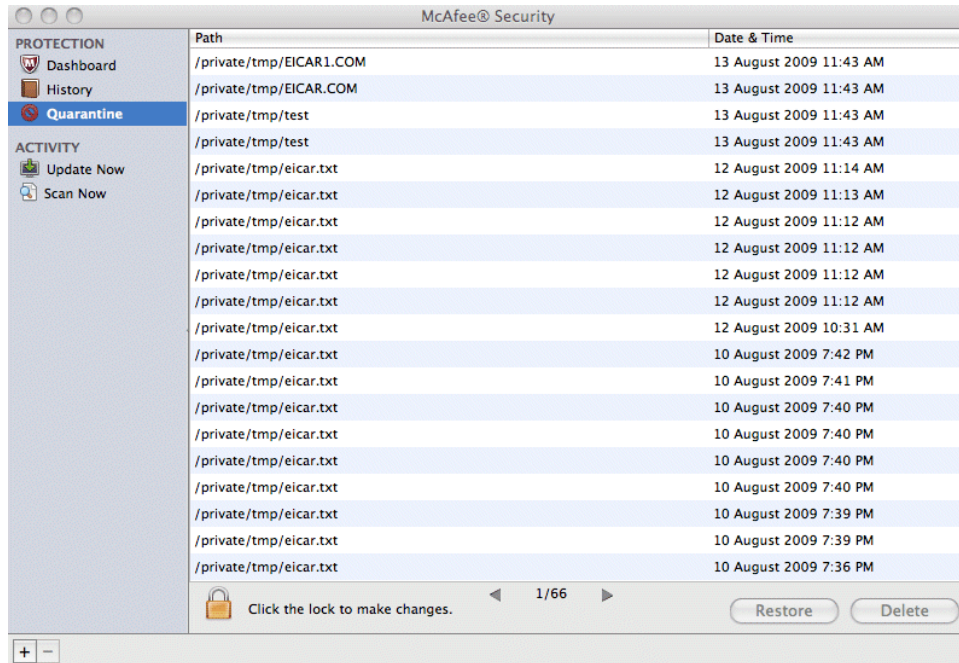
To remove an event, click the event, then click **Delete** (or press **delete**). You can also select multiple events, then click **Delete** (or press **delete**). To delete all the events from the **History** screen, click **History** on the **McAfee Security** menu bar, then select **Clear history**.

NOTE: You must have administrator rights delete event(s) or clear the history of events.

Quarantining malware

The quarantine functionality enforces an item (suspected of containing malware) to isolate to a quarantine location that you specified while installing McAfee Security, so that the item cannot be opened or executed.

The **Quarantine** screen displays the original location of items that are quarantined and the instance when they were quarantined. You can use the arrows at the bottom of the console to navigate through multiple **Quarantine** pages.



Restoring and deleting quarantined item

Select a path and click **Restore** to restore the item to its original location. Click **Delete** (or press **delete**) to remove the quarantined item.

NOTE: You must have administrator rights to restore or delete a quarantined item.

Default activities in McAfee Security Console

On launching the McAfee Security console, you can use the following default activities:

- ▶ [Update Now](#)
- ▶ [Scan Now](#)

Update Now

This option helps you manually run an Update to keep your Mac up-to-date with the latest anti-malware DAT and Engine.

- 1 Click **Update Now** on the left pane of the console. Alternatively, you can click **Activity | Start Anti-malware Update** from the **McAfee Security** menu bar.
- 2 Click **Start Update** to initiate the anti-malware update task.
After the update process is complete, the details of the update process are displayed, which includes the latest DAT and Engine versions, status of the last update, and the DAT creation date.

TIP: You can view the details of the Update task on the **History** screen.

Scan Now

This option helps you scan specific files, folders, local or network mounted volumes, and other items on your Mac immediately.

- 1 Click **Scan Now** on the left pane of the console.
- 2 In the **What to scan** section, select the items from the drop-down menu. Click **+** to include more items to be scanned.
Alternatively, you can drag-and-drop files for scanning.
- 3 Click **Start Scan**. A progress bar appears indicating the items being scanned. After scanning completes, a summary of the scan task is displayed, which includes the number of items scanned and threats detected.

TIP: You can view the details of the scan task on the **History** screen.

Configuring scan tasks

Use the following instructions in this section to create, modify, and delete scan tasks.

Tasks

- ▶ [Creating a new scan task](#)
- ▶ [Modifying an existing scan task](#)
- ▶ [Deleting a scan task](#)

Creating a new scan task

Use this task to create and run regular scan operations as required.

- 1 Launch the McAfee Security Console.
NOTE: For instructions, see the *Launching McAfee Security Console* section.
- 2 Click **+** on the bottom left corner of the McAfee Security console. Alternatively, you can press **command + N** or you can click **Activity | New Activity** on the **McAfee Security** menu bar.
- 3 Type a **Scan Name**, then click **Create**. The scan task name appears on the left pane.
- 4 In the **What to scan** section, select the items from the drop-down menu. Alternatively, you can drag-and-drop items for scanning.
- 5 In the **When to scan** section, select an appropriate schedule for the scan task.
NOTE: If you select to scan items immediately, click **Start Scan**.
- 6 Click **Schedule Scan**. A message appears stating that the scan task is scheduled.
- 7 Click **OK**.

Modifying an existing scan task

Use this task to modify an existing scan task.

- 1 Click on an existing scan task name on the left pane of the console.

- 2 If the existing scan task is:
 - Scheduled task — Click **Modify Task** , select the required items for scanning, re-schedule the scan as required, then click **Schedule Scan**.
 - Scheduled to run immediately — To run this task immediately, select the required items for scanning, then click **Start Scan**.
 - Scheduled to run immediately — To re-schedule this task, select the required items for scanning, then click **Schedule Scan**.

Deleting a scan task

Use this task to delete a scan task.

- 1 Click on an existing scan task name on the left pane of the console.
- 2 Perform one of the following steps:
 - Click - on the left bottom corner of the console.
 - Click **Activity | Delete Activity** from the **McAfee Security** menu bar.
 - Press **delete**.

Configuring McAfee Security Preferences

McAfee Security preferences enable you to configure the anti-malware and update preferences.

Prerequisite: You must have administrator rights to configure McAfee Security preferences.


Topics covered in this chapter are:

Contents

- ▶ General Preferences
- ▶ Configuring Anti-malware Preferences
- ▶ Enhanced Notification Report
- ▶ Update Preferences
- ▶ Default Preferences
- ▶ Help option in the menu bar

General Preferences

General preferences allow you to enable or disable on-access scan.

- 1** Click the McAfee menulet  on the status bar, then select **McAfee Security Preferences**. Alternatively, you can launch the McAfee Security Console, then perform one of the following instructions:
 - Click **McAfee Security** on the menu bar, then select **Preferences**.
 - Press **Command+**,
The **General** screen appears.

NOTE: For instructions on launching the McAfee Security console, see the *Launching McAfee Security console* section.
- 2** Click the lock to make changes. Type your administrator password when prompted, then click **OK**.
- 3** Click **ON** or **OFF** to enable or disable the following feature:
 - **On-access Scan**

Configuring Anti-malware Preferences

Anti-malware preferences enable you to configure the on-access scan and on-demand scan preferences, and specify items to be excluded from scanning. You can even specify regular expression based exclusions for on-access and on-demand scanning separately.


NOTE: Click **Reset** to reset the anti-malware preferences to their default values.

To configure the anti-malware preferences, perform the following instructions in this section.

- ▶ [Configuring On-access Scan Preferences](#)
- ▶ [Configuring On-demand Scan Preferences](#)
- ▶ [Specifying Anti-malware Exclusions](#)

Configuring On-access Scan Preferences

Use this task to configure on-access scan preferences. On-access scan consistently monitors all items for malware. On-access scanning takes place whenever an item is read from the disk, written to the disk (or both) based on the configured preferences.

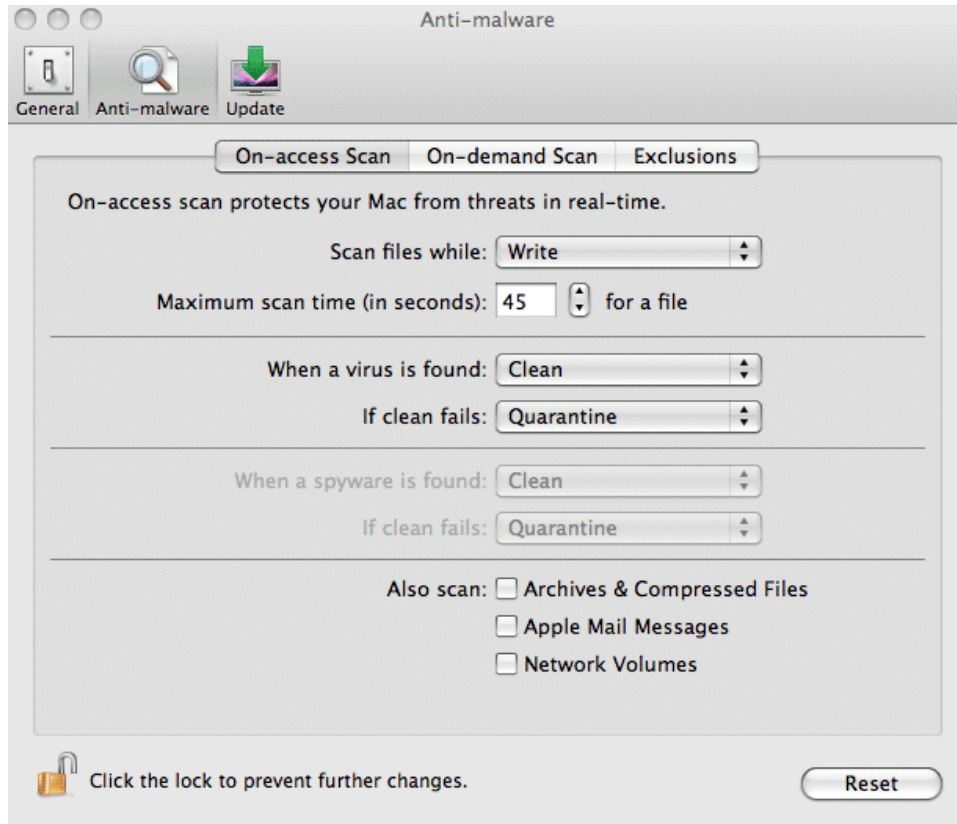
1 Click the McAfee menulet  on the status bar, then select **McAfee Security Preferences**. Alternatively, you can launch the McAfee Security Console, then perform one of the following instructions:

- Click **McAfee Security** on the menu bar, then select **Preferences**.
- Press **Command+**,

2 Click **Anti-malware**.

NOTE: By default, the **On-access Scan** preferences screen is displayed.

3 To configure the on-access scan preferences, click the lock, type your administrator password, then click **OK**. The on-access scan preferences will have default settings.




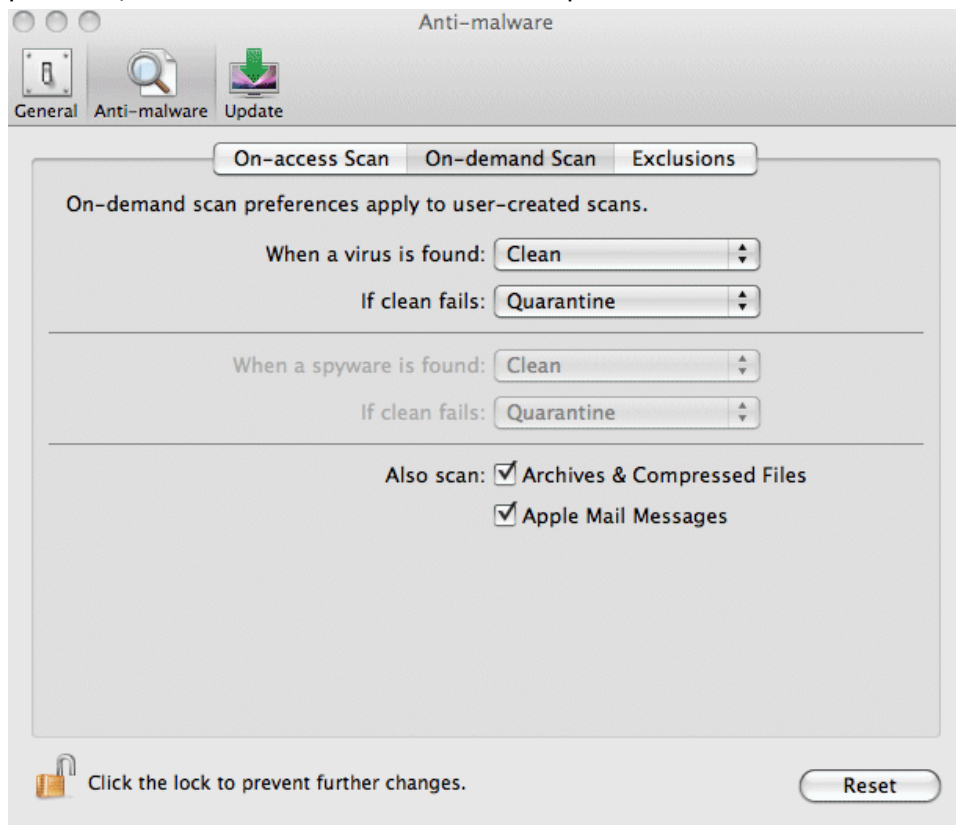
- 4 Use the following options to configure the on-access scan preferences:
- From the **Scan files while** drop-down menu, select one of the following options:
 - **Read** — To scan items that are only being read from the hard disk.
 - **Write** — To scan items when they are written to the hard disk.
 - **Read & Write** — To scan items that are being read from or written to the hard disk.
 - In **Maximum scan time (in seconds)**, specify a time after which the scanning of each file terminates. The minimum and maximum values you can specify are 10 and 999 seconds respectively. Default value is 45 seconds.
 - From the **When a virus is found** drop-down menu, select one of the following options:
 - **Clean** — To clean (repair) the virus. If you select this option, the If clean fails drop-down menu appears, which provides you the options to quarantine or delete the item (infected with virus) or notify you of the virus detection, when the cleaning process fails.
 - **Quarantine** — To quarantine the item containing virus. If you select this option, the If quarantine fails drop-down menu appears, which provides you the options to delete the item (infected with virus) or notify you of the virus detection, when the quarantine process fails.
 - **Delete** — To delete the item containing virus.
 - **Notify** — To notify you in case of a virus detection (no other actions being taken).
 - You can also enable scanning for:
 - **Archives & Compressed Files**
 - **Apple Mail Messages**

- **Network Volumes**

Configuring On-demand Scan Preferences

Use this task to configure on-demand scan preferences. You can schedule on-demand scans to run immediately, at a particular time, or at regular intervals.

- 1 Click the McAfee menulet  on the status bar, then select **McAfee Security Preferences**. Alternatively, you can launch the McAfee Security Console, then perform one of the following instructions:
 - Click **McAfee Security** on the menu bar, then select **Preferences**.
 - Press **Command+**,
- 2 Click **Anti-malware**.
- 3 Click **On-demand Scan**.
- 4 To configure the on-demand scan preferences, click the lock, type your administrator password, then click **OK**. The on-demand scan preferences will have default settings.




- 5 Use the following options to configure the on-demand scan preferences:
 - From the **When a virus is found** drop-down menu, select one of the following options:
 - **Clean** — To clean (repair) the virus. If you select this option, the If clean fails drop-down menu appears, which provides you the options to quarantine or delete the item (infected with virus) or notify you of the virus detection, when the cleaning process fails.
 - **Quarantine** — To quarantine the item containing virus. If you select this option, the If quarantine fails drop-down menu appears, which provides you the options to

delete the item (infected with virus) or notify you of the virus detection, when the quarantine process fails.

- **Delete** — To delete the item containing virus.
- **Notify** — To notify you in case of a virus detection (no other actions being taken).
- You can also enable scanning for:
 - **Archives & Compressed Files**
 - **Apple Mail Messages**

Specifying Anti-malware Exclusions

Use this task to specify anti-malware exclusions. You can exclude specific items from being scanned.

- 1** Click the McAfee menulet  on the status bar, then select **McAfee Security Preferences**. Alternatively, you can launch the McAfee Security Console, then perform one of the following instructions:
 - Click **McAfee Security** on the menu bar, then select **Preferences**.
 - Press **Command+**,
- 2** Click **Anti-malware** then click **Exclusions**.
- 3** Click the lock to make changes. Type your administrator password when prompted, then click **OK**.
- 4** Click **+** at the bottom left corner of the screen. The **Set Exclusions** screen appears allowing you to select and add items to the exclusion list.
- 5** Select the required items, then click **OK** to return to the **Exclusions** screen.
- 6** Select or deselect the **On-access Scan** and/or **On-demand Scan** options as required. By default, both options are enabled so that the items are excluded from both the scans.

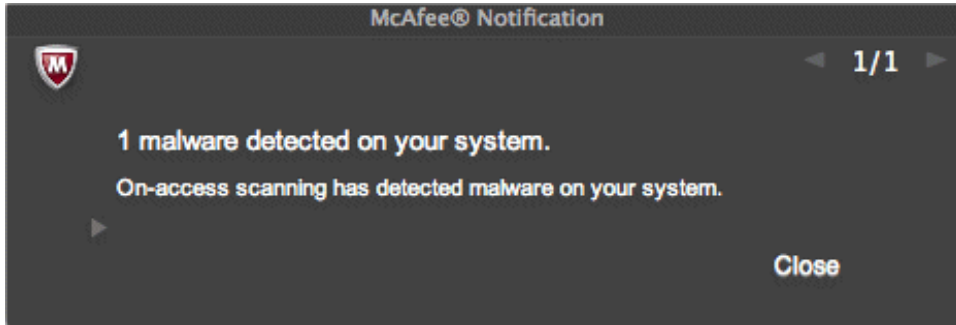
NOTE: To modify the path/item of an existing exclusion, double-click it in the corresponding cell. The path/item becomes editable. Specify the new path/item. You can also specify regular expression based exclusions.

To delete an exclusion, select it, then click **-** at the bottom left corner of the screen (or press **delete**).

Enhanced Notification Report

McAfee Security notifies you of the following scenarios in an enhanced **McAfee Notification** screen:


- Malware detected during on-access scanning. (Click the caret to find the detection details).



Update Preferences

McAfee Security is configured to access the McAfee FTP server, HTTP server and/or a local repository to download the latest DAT files. After installing McAfee Security, it automatically connects to a FTP, HTTP and/or a local repository (that you have configured) to download and update your DAT files while you are connected to the Internet.

If your organization uses proxy servers to connect to the Internet for retrieving packages, you can use the **Proxy Settings** tab.

- 1** Click the McAfee menulet  on the status bar, then select **McAfee Security Preferences**. Alternatively, you can launch the McAfee Security Console, then perform one of the following instructions:
 - Click **McAfee Security** on the menu bar, then select **Preferences**.
 - Press **Command+**,
- 2** Click **Update**.
- 3** To configure the update preferences, click the lock, type your administrator password, then click **OK**. The Update preferences will have default settings.

By default, the **Repository List** screen opens.
- 4** In **Repository name**, you can use:
 - **+** : to add a new repository. Click **+** on the bottom left corner of the screen and type a name for the new repository.
 - **-** : to delete an existing repository that you create. Select a repository, click **-** on the bottom left corner of the screen or press **delete**.
 - **^ v** : to prioritize repositories. You can even drag-and-drop the repositories to prioritize them.
- 5** In **Repository Type**, select **FTP**, **HTTP**, or a **Local** repository from where the latest DATs can be downloaded.
- 6** Specify a **Repository URL**, **Port**, **User Name**, and **Password** for the repository.
- 7** Click **Proxy Settings**.

NOTE: Click **Do not use a proxy** if you do not want to use a proxy server for connecting to the Internet.
- 8** To use a proxy server, click **Configure proxy settings manually**.

- 9 To specify the same IP address and port number for all the proxy types, select the **Use these settings for all proxy types** option.
- 10 Select **FTP** or **HTTP** server as required. Type the IP **Address** and **Port** number of the selected server.
- 11 To specify username and password for FTP, HTTP, or a local repository, select the **Use authentication** option.
- 12 To bypass a proxy server for specific domain(s), select the **Specify exceptions** option, then type the proxy server name.
- 13 Click the **Schedule** tab and schedule the task as required.
- 14 Click **Apply**.

Default Preferences

Features	Default preferences
Anti-malware	On-access Scan: <ul style="list-style-type: none">• Scan on write — Enabled.• Maximum scan time for a file — 45 seconds.• When a virus is found,<ul style="list-style-type: none">• Primary action — Clean.• If primary action fails — Quarantine.• Scan archives and compressed files — Disabled.• Scan Apple Mail messages — Disabled.• Scan network volumes — Disabled.
	On-demand Scan: <ul style="list-style-type: none">• Scan archives and compressed files — Enabled.• Scan Apple Mail messages — Enabled.
Update	<ul style="list-style-type: none">• Repository — McAfeeHttp, McAfeeFtp.• Proxy settings — Do not use a proxy.

NOTE: You must have administrator rights to configure/modify McAfee Security preferences.

Help option in the menu bar

After launching McAfee Security, you can use the following options by clicking **Help** on the menu bar:

McAfee Security Help

Selecting this option helps you access the help pages of McAfee Security that provides high-level and detailed instructions on how to use the software.

RUN MERTool

MER tool helps you collect the diagnostic data of McAfee Security. Selecting this option prompts you to type your administrator password. Once you type your password, a diagnostic report of all logs **McAfeeMERTool.zip** is created and located in your home directory.

McAfee Support

Selecting this option opens the McAfee Enterprise Support webpage that provides information on McAfee Technical Support.

McAfee KnowledgeBase

Selecting this option opens the McAfee Technical Support ServicePortal webpage where the corporate knowledge base articles are published.

McAfee HotFixes / Patches

Selecting this option opens the McAfee Technical Support ServicePortal webpage from where you can download the product hotfixes and patches.

Submit A Malware Sample

Selecting this option opens the McAfee Avert(r) Labs WebImmune webpage where you can submit potentially infected files to WebImmune for analysis.

McAfee Virus Information Lab

Selecting this option opens the McAfee Avert Labs Threat Library webpage that has detailed information on the origin of viruses, Trojans, hoaxes, vulnerabilities and potentially unwanted programs.

Index

A

anti-malware feature
testing 8

C

check-in Agent package
ePO 4.5 15
check-in McAfee Security package
ePO 4.5 15
command-line installation 8
configure
scan task 24
configure preferences
on-access scanner 27
on-demand scanner 29
create
on-demand scan task 24
create new policy 12
create policies
ePO 4.5 17

D

dashboard 20
default activity
scan now 24
update now 23
delete
on-demand scan task 25
detection reports 30

E

enforce policies
ePO 4.0 12
ePO 4.0
check-in McAfee Agent package 11
check-in McAfee Security package 11
enforce policies 12
install McAfee Agent on clients 11
schedule scan 13
schedule task 13
setting up policies 12
uninstall mcafee security 13
ePO 4.5
install McAfee Security 15
schedule task 18
setting policies 17
uninstall mcafee security from client 19
ePO4.0
remove extensions 14
remove product from client 14
ePO4.5
create policies 17
policy enforcement 18

exclusions
scanning 30

F

files
exclude from scanning 30

G

general preferences 26

H

help option
menubar 32
history
all product events 21
History screen 21

I

install
extensions 11, 16
install McAfee Agent
using ePO 4.0 11
install McAfee Agent on client
using ePO 4.5 16
install McAfee Security
ePO 4.5 10
using ePO 4.5 15
install McAfee Security on client
using ePO 4.5 17
installation methods 7
integration with ePO 4.0
prerequisites 10
introduction
McAfee Security 5

L

launch
Mcafee Security console 20

M

malware
quarantine 22
McAfee Alert 30
McAfee Notification 30
McAfee Security
how it works 5
install on client computers 12
installation 7
integrating with ePO 4.0 10
integrating with ePO 4.5 15
introduction 5
launch console 20

McAfee Security (*continued*)
 methods of installing [7](#)
 new features [5](#)
 preferences [26](#)
 prerequisites for installing [7](#)
 uninstall [9](#)
 McAfee Security dashboard [20](#)
 McAfee Security extensions
 install [11](#), [16](#)
 menubar option
 help [32](#)
 modify
 on-demand scan task [24](#)
 scan task [24](#)

N

new policy
 create using ePO [12](#)

O

on-access scanner
 configure preferences [27](#)
 on-demand scan
 schedule using ePO 4.0 [13](#)
 on-demand scan task
 create [24](#)
 delete [25](#)
 modify [24](#)
 on-demand scanner
 configure preferences [29](#)

P

policies
 ePO 4.0 [12](#)
 policy enforcement
 ePO 4.5 [18](#)
 preferences [26](#), [27](#)
 anti-malware [27](#)
 prerequisites [7](#), [10](#)
 integration with ePO 4.0 [10](#)
 product
 new features [5](#)

Q

quarantine
 malware [22](#)

R

remove extension
 ePO 4.0 [14](#)
 remove McAfee Security extensions
 ePO 4.5 [19](#)
 reports
 McAfee Alert [30](#)
 McAfee Notification [30](#)

S

scan now [23](#), [24](#)
 scan task
 modify [24](#)
 scanner
 exclusions [30](#)
 schedule scan [24](#)
 schedule tasks
 using ePO 4.0 [13](#)
 using ePO 4.5 [18](#)
 set policies
 ePO 4.5 [17](#)
 silent installation [8](#)
 standard installation [8](#)
 system requirements [7](#)

T

testing
 anti-malware feature [8](#)

U

uninstall
 McAfee Security [9](#)
 mcafee security using ePO 4.0 [13](#)
 uninstall mcafee security
 from client [14](#)
 uninstall McAfee Security
 ePO 4.5 [18](#)
 uninstall mcafee security from client
 ePO 4.5 [19](#)
 update now [23](#)

W

what's new [5](#)

