Product Guide

McAfee VirusScan for Mac 9.6.0
COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

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

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>5</td>
</tr>
<tr>
<td>About this guide</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>Conventions</td>
<td>5</td>
</tr>
<tr>
<td>Find product documentation</td>
<td>6</td>
</tr>
<tr>
<td><strong>1 Introduction</strong></td>
<td>7</td>
</tr>
<tr>
<td>Why you need security for Mac</td>
<td>7</td>
</tr>
<tr>
<td>How McAfee VirusScan for Mac protects your system</td>
<td>8</td>
</tr>
<tr>
<td>Anti-malware</td>
<td>8</td>
</tr>
<tr>
<td>Product features</td>
<td>8</td>
</tr>
<tr>
<td><strong>2 Installation and deployment</strong></td>
<td>11</td>
</tr>
<tr>
<td>System requirements</td>
<td>11</td>
</tr>
<tr>
<td>Package contents</td>
<td>12</td>
</tr>
<tr>
<td>Install the software on a standalone Mac</td>
<td>12</td>
</tr>
<tr>
<td>Install the software using wizard</td>
<td>12</td>
</tr>
<tr>
<td>Install the software from the command line (silent installation)</td>
<td>12</td>
</tr>
<tr>
<td>Upgrade the software</td>
<td>13</td>
</tr>
<tr>
<td>Upgrade the software on a standalone Mac</td>
<td>13</td>
</tr>
<tr>
<td>Upgrade the software on a managed Mac</td>
<td>13</td>
</tr>
<tr>
<td>Default settings</td>
<td>14</td>
</tr>
<tr>
<td>Recommended post-installation tasks</td>
<td>15</td>
</tr>
<tr>
<td>Deploy the software on a managed Mac</td>
<td>16</td>
</tr>
<tr>
<td>Check in the package using software manager</td>
<td>16</td>
</tr>
<tr>
<td>Install the extensions using software manager</td>
<td>16</td>
</tr>
<tr>
<td>Check in the package manually</td>
<td>17</td>
</tr>
<tr>
<td>Install the extensions manually</td>
<td>17</td>
</tr>
<tr>
<td>Deploy McAfee VirusScan for Mac from ePolicy Orchestrator</td>
<td>17</td>
</tr>
<tr>
<td>Test the installation</td>
<td>18</td>
</tr>
<tr>
<td>Test the anti-malware protection feature</td>
<td>18</td>
</tr>
<tr>
<td>Uninstall the software</td>
<td>19</td>
</tr>
<tr>
<td>Uninstall the software from a standalone Mac</td>
<td>19</td>
</tr>
<tr>
<td>Remove the software from a managed Mac</td>
<td>19</td>
</tr>
<tr>
<td><strong>3 Using the software on a standalone Mac</strong></td>
<td>21</td>
</tr>
<tr>
<td>Dashboard</td>
<td>21</td>
</tr>
<tr>
<td>Security status</td>
<td>21</td>
</tr>
<tr>
<td>Recent events summary</td>
<td>21</td>
</tr>
<tr>
<td>History of events</td>
<td>22</td>
</tr>
<tr>
<td>Quarantine malware</td>
<td>22</td>
</tr>
<tr>
<td>Remove or restore the quarantined item</td>
<td>22</td>
</tr>
<tr>
<td>Update the anti-malware and DAT files</td>
<td>23</td>
</tr>
<tr>
<td>Perform a system scan</td>
<td>23</td>
</tr>
<tr>
<td>Configure custom scan tasks</td>
<td>23</td>
</tr>
</tbody>
</table>
Create a scan task ........................................... 24
Modify an existing scan task ................................. 25
Remove an existing scan schedule ......................... 25

4 Configuring protection preferences on a standalone Mac 27
General preferences ........................................... 27
  Configure general preferences .............................. 27
Anti-malware ................................................... 28
  Configure on-access scan preferences ...................... 28
  Configure on-demand scan preferences ...................... 29
Define anti-malware exclusions ............................. 29
  Best practices for anti-malware preferences ................ 30
Configure an update schedule ............................... 31
  Configure the repository list .............................. 31
  Configure proxy settings ................................. 32
  Configure the anti-malware update schedule ............ 32

5 Managing the software with ePolicy Orchestrator 35
Manage policies .............................................. 35
  Create or modify policies ................................ 35
  Assign policies .......................................... 36
Create a self-protection policy ............................. 36
Create an anti-malware policy ............................... 37
Schedule an anti-malware update ........................... 39
Schedule an on-demand scan ............................... 40
Queries and reports ........................................ 41
  Run a query ............................................. 41

6 Troubleshooting 43
Run the repairMSC utility ................................... 43

Index 45
Preface

This guide provides the information you need for all phases of product use, from installation to configuration to troubleshooting.

Contents

- About this guide
- Find product documentation

About this guide

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

Audience

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

The information in this guide is intended primarily for:

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

Conventions

This guide uses these typographical conventions and icons.

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

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

**Task**


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

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1. Click <strong>Product Documentation</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Select a product, then select a version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click <strong>Search the KnowledgeBase</strong> for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Browse the KnowledgeBase</strong> for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introduction

McAfee® VirusScan® for Mac offers scalable security solution that minimizes the risk of exposing your Mac to vulnerabilities.

The software provides a securely configured environment that:

- Protects your Mac from viruses, spyware, trojan horses, and other malware threats.

Contents

- Why you need security for Mac
- How McAfee VirusScan for Mac protects your system
- Product features

Why you need security for Mac

Systems without protection may result security breach in many ways such as data loss, misuse of personal and business information, and system disorder.

New products and technologies broaden opportunities for new security threats and challenges. The motive behind these threats is to interrupt and espionage your system or destruct the data and the system functionality completely.

The targeted security threats devised by cyber criminals and hackers are evolving consistently and increasing the risk consistently. The analyst reports say that the overall malware samples reached more than a 100 million implying the importance of securing your Mac from the threats.

The list of threats and reported vulnerabilities that can harm your Mac are:

<table>
<thead>
<tr>
<th>Threat category</th>
<th>Potential threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Directs the user to access malicious items that can infect a Mac.</td>
</tr>
<tr>
<td></td>
<td>Examples: Flashback Trojan, Fake AV</td>
</tr>
<tr>
<td>Spyware</td>
<td>Tracks every key you type to access sensitive information, such as user name and password and other personal details.</td>
</tr>
<tr>
<td></td>
<td>Example: Keyloggers</td>
</tr>
</tbody>
</table>

With McAfee VirusScan for Mac is enabled, your Mac is protected from these malware threats without compromising the needs. The software also provides a secured environment that eliminates the risk to exposing to these vulnerabilities.
How McAfee VirusScan for Mac protects your system

McAfee VirusScan for Mac provides a comprehensive security mechanism that includes anti-malware and anti-spyware protection.

Anti-malware

Anti-malware protection secures your Mac from malware threats proactively with the predefined actions upon detecting malware and suspicious items.

When enabled, the anti-malware feature scans files, folders on local, network-mounted volumes, and removable media whenever you create or access an item.

The anti-malware engine:

- Performs complex analysis using the malware definition files (DATs)
- Decodes the contents of the item you access
- Compares them with the known signatures stored in the DAT files to identify malware

For more information, see Anti-malware preferences.

Product features

The main features of McAfee VirusScan for Mac are described in this section.

Anti-malware

- Anti-spyware protection — Protects the Mac from spyware threats.
- On-access Scan — Scan files and folders whenever users access them.
- Performance improvements for On-demand-Scan (ODS) — Completes scan files and folders faster with less resource.
- Quarantine — Quarantine malware items (or suspected malware-like behavior) so that they can't be opened or executed.
- Schedule Scan — Define schedules to scan files and folders on local and mounted volumes.
- Separate regular expression based exclusion for on-access scan and on-demand scan.
- Scan network volume, compressed files, and emails.

Interface

- McAfee menulet for easy access — Access the McAfee menulet 🔄 to launch the McAfee VirusScan for Mac Console, McAfee VirusScan for Mac Preferences, and the About McAfee Endpoint Protection for Mac dialog box.
- Dashboard — View the security status of your Mac, scheduled scan tasks, latest events, and the anti-malware update details.
- History of events — View all anti-malware events.
- Notifications — McAfee Notification displays:
  - Detection of malware (resulting from on-access scan)
General

- **Self protection** — Allows ePolicy Orchestrator administrators to enable password protection in the client interface to prevent local users from modifying the defined policy preferences, and to uninstall the software on managed Macs.
Installation and deployment

Install McAfee VirusScan for Mac on a standalone (unmanaged) Mac, or deploy from ePolicy Orchestrator on a managed Mac.

McAfee VirusScan for Mac is synonym of the anti-malware component of McAfee Endpoint Protection for Mac. Therefore, when you install McAfee VirusScan for Mac, you will notice the product name appears as McAfee Endpoint Protection for Mac in the user interface, ePolicy Orchestrator, and in the extension packages.

Contents

- System requirements
- Package contents
- Install the software on a standalone Mac
- Upgrade the software
- Default settings
- Recommended post-installation tasks
- Deploy the software on a managed Mac
- Test the installation
- Uninstall the software

System requirements

Make sure that your Mac meets these requirements and that you have administrator rights.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>• Lion 10.7.x and later</td>
</tr>
<tr>
<td></td>
<td>• Mountain Lion 10.8.x and later</td>
</tr>
<tr>
<td></td>
<td>• Mavericks 10.9 and above</td>
</tr>
<tr>
<td></td>
<td>• Mac OS X server</td>
</tr>
<tr>
<td>Hardware</td>
<td>Mac that can run with the supported operating system configuration.</td>
</tr>
<tr>
<td>McAfee management software</td>
<td>McAfee ePolicy Orchestrator 4.6.x and 5.0.x.</td>
</tr>
<tr>
<td>McAfee Agent (required for ePolicy Orchestrator deployment)</td>
<td>McAfee Agent for Mac 4.8 Patch 1 and later.</td>
</tr>
</tbody>
</table>
Installation and deployment

Package contents

The software package contains these files that are necessary for installation.

<table>
<thead>
<tr>
<th>Package</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSM&lt;version&gt;-&lt;release-type&gt;-&lt;build-number&gt;.dmg</td>
<td>Contains files to install the software on standalone Mac.</td>
</tr>
<tr>
<td>VSM&lt;version&gt;-&lt;release-type&gt;-ePO-&lt;build_number&gt;.zip</td>
<td>Contains files to deploy the software from the ePolicy Orchestrator server.</td>
</tr>
</tbody>
</table>

Install the software on a standalone Mac

Install the software on a standalone Mac using the wizard or from the command line.

Tasks

- **Install the software using wizard** on page 12
  The wizard guides you through the steps to install the software on your Mac.

- **Install the software from the command line (silent installation)** on page 12
  You can use the command line to install the software without user intervention.

Install the software using wizard

The wizard guides you through the steps to install the software on your Mac.

When the installation is complete, McAfee VirusScan for Mac starts protecting your system immediately. Any existing network connections on your Mac are disconnected. You must re-establish those connections.

Task

1. Download VSM<version>-<release-type>-<build-number>.dmg to a temporary location on your Mac, then double-click it to mount VSM<version>-<release-type>-<build-number>.pkg.

2. Double-click VSM<version>-<release-type>-<build-number>.pkg to open the wizard.

3. Follow the prompts to install the software.

Install the software from the command line (silent installation)

You can use the command line to install the software without user intervention.

When the installation is complete, the software starts protecting your Mac immediately. Any existing network connections that are running on your Mac are disconnected. You must re-establish those connections.

Task

1. Download VSM<version>-<release-type>-<build-number>.dmg, then double-click it to mount VSM<version>-<release-type>-<build-number>.pkg file.

2. Copy the VSM<version>-<release-type>-<build-number>.pkg file to a temporary location on your Mac.

3. Open a Terminal window and change the working directory to the one where you saved the VSM<version>-<release-type>-<build-number>.pkg file.
4 Type the following command, then press return.
   `sudo installer -pkg VSM<version>-<release-type>-<build-number>.pkg -target /`

5 Type the administrator password, then press return. The following message appears.

```
The Install was successful.
```

---

### Upgrade the software

McAfee VirusScan for Mac supports upgrading the software and migrating the configuration from the previous versions of the software.

#### Upgrade the software on a standalone Mac

You can upgrade the software and migrate the existing configuration settings.

You can upgrade the software from:

- McAfee VirusScan for Mac 9.1 and later to McAfee VirusScan for Mac 9.6
  
  When the software is upgraded, the Anti-malware preferences and rules are migrated during the upgrade.

Before upgrading the software, make sure that these system requirements are met:

- Operating system
- ePolicy Orchestrator
- McAfee Agent

If the minimum required version of McAfee Agent is not found in the Mac during the upgrade, the installation program upgrades McAfee Agent also.

When a previous version of the software is found during the installation, the installation program upgrades the software to the new version. To upgrade the software:

1 Install the software using the wizard.
   
   For more information, see Install the software using wizard.

2 Make sure that all existing rules and preferences are migrated to the new version.

#### Upgrade the software on a managed Mac

When you upgrade the extension, the existing policies are migrated and the existing reports are upgraded to the new version.

You can upgrade the software from:

- McAfee VirusScan for Mac 9.1 and later to McAfee VirusScan for Mac 9.6
  
  When the software is upgraded, the Anti-malware policies are migrated and these policies will co-exist with the new policies.

Before upgrading the software, make sure that the system requirements are met:
• Operating system
• ePolicy Orchestrator
• McAfee Agent

If the minimum required version of McAfee Agent is not found in the managed Mac, the upgrade will fail.

Make sure that you take a backup of existing policies for the existing version of the product. For instructions about backing up policies, see the ePolicy Orchestrator product guide of your version.

When the Anti-malware only extension is migrated, the anti-spyware default settings are applied.

ePolicy Orchestrator reports extensions are upgraded and events from the earlier version can be used for queries. After migration, all the queries from the earlier version are available under the new version.

1 Check in and deploy the extension.
   For more information, see check in the package and install the extensions.

2 Make sure that the policies are migrated properly and the reports are upgraded to the new version.

3 Deploy the product.

Default settings

Once installed, McAfee VirusScan for Mac starts protecting the Mac immediately based on the default configurations defined. Refer to these default settings, and configure them for your environment.

Anti-malware

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>On-access Scan — On&lt;br&gt;Spyware Scan — On</td>
</tr>
<tr>
<td>Anti-malware</td>
<td>On-access Scan:&lt;br&gt;• Scan files while — Write&lt;br&gt;• Maximum scan time for a file — 45 seconds for a file.&lt;br&gt;• When a virus is found — Clean&lt;br&gt;• If clean fails — Quarantine&lt;br&gt;• When a spyware is found — Clean&lt;br&gt;• If clean fails — Quarantine&lt;br&gt;Also scan:&lt;br&gt;• Archives &amp; Compressed Files — Disabled&lt;br&gt;• Apple Mail messages — Disabled&lt;br&gt;• Network Volumes — Disabled</td>
</tr>
</tbody>
</table>
### Recommended post-installation tasks

Perform these tasks to keep the anti-malware and DAT files up to date, and to make sure that the protection configuration does not affect the business routines.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update anti-malware and DAT files</td>
<td>After installation, McAfee VirusScan for Mac automatically updates the DAT files to protect the Mac from the latest threats. By default, this update is scheduled at 4.45 pm local time every day. When the DAT files are updated for the first time, it may take longer time to download the full DAT. The subsequent updates will be incremental.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Update the anti-malware and DAT files.</td>
</tr>
<tr>
<td>Perform an on-demand scan</td>
<td>Run an on-demand-scan to scan the local volumes, after you install the software to clean the infected files that are not accessed by but reside in the Mac.</td>
</tr>
<tr>
<td>Anti-malware protection</td>
<td>McAfee VirusScan for Mac comes with the default settings for anti-malware protection. Verify that the default settings are consistent with your organization policies and provides complete protection against malware.</td>
</tr>
<tr>
<td></td>
<td>Configure the On-demand Scan task to define:</td>
</tr>
<tr>
<td></td>
<td>• The items to scan (files, folders, and drives)</td>
</tr>
<tr>
<td></td>
<td>• Set frequency of scan (daily, weekly, monthly, or immediately)</td>
</tr>
<tr>
<td></td>
<td>• Define the action when malware is found (<a href="#">Delete</a> or <a href="#">Quarantine</a>)</td>
</tr>
<tr>
<td></td>
<td>For more information, see Configure protection preferences.</td>
</tr>
</tbody>
</table>
Deploy the software on a managed Mac

Deploy McAfee VirusScan for Mac remotely to a client system in your network using ePolicy Orchestrator. You can check in and install the packages and extensions in two ways:

- Check in the package and extension using Software Manager.
- Check in the package and extensions manually.

Tasks

- **Check in the package using software manager on page 16**
  You can check in, update, and remove McAfee VirusScan for Mac using the Software Manager.

- **Install the extensions using software manager on page 16**
  You can install the extensions using the Software Manager.

- **Check in the package manually on page 17**
  Check in the McAfee VirusScan for Mac deployment package to the ePolicy Orchestrator master repository.

- **Install the extensions manually on page 17**
  Install McAfee VirusScan for Mac extensions using ePolicy Orchestrator.

- **Deploy McAfee VirusScan for Mac from ePolicy Orchestrator on page 17**
  Use ePolicy Orchestrator to deploy the software to systems in your network that are managed.

Check in the package using software manager

You can check in, update, and remove McAfee VirusScan for Mac using the Software Manager.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator as an administrator.

2. Click Menu, Software, then click Software Manager.

3. In the Software Manager page Product Categories list, select Software (By Label), select McAfee Endpoint Protection for Mac 2.1, select VSM<version>-<release-type>-ePO<-build_number>, then click Check in All.

Install the extensions using software manager

You can install the extensions using the Software Manager.

Task

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator as an administrator.

2. Click Menu, Software, then click Software Manager.

3. In the Software Manager page Product Categories list, select Software (By Label), select McAfee Endpoint Protection for Mac 2.1, select the following extensions, then click Check in All:
   - Endpoint Protection for Mac 2.1.0:Anti-malware
   - Endpoint Protection for Mac 2.1.0:General
   - Endpoint Protection for Mac 2.1.0:Anti-malware Reporter
Check in the package manually
Check in the McAfee VirusScan for Mac deployment package to the ePolicy Orchestrator master repository.

Task
For option definitions, click ? in the interface.

1. Download the VSM<version>-<release-type>-ePO-<build_number>.zip file to a temporary location on the ePolicy Orchestrator server.
2. Log on to the ePolicy Orchestrator server as an administrator.
3. Click Menu | Software | Master Repository, then click Action | Check In Package.
   a. For Package type, select Product or Update (.ZIP).
   b. Click Choose File, select VSM<version>-<release-type>-ePO-<build_number>, click Choose, then click Next.
4. Select Current, then click Save.

Install the extensions manually
Install McAfee VirusScan for Mac extensions using ePolicy Orchestrator.
You must install these extensions to enable the features of the product:

- Endpoint Protection for Mac 2.1.0: Anti-malware
- Endpoint Protection for Mac 2.1.0: General
- Endpoint Protection for Mac 2.1.0: Anti-malware Reporter

Task
For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click Menu | Software | Extensions, then click Install Extension.
3. Click Choose File and select the file that contains the extension, then click OK.

Deploy McAfee VirusScan for Mac from ePolicy Orchestrator
Use ePolicy Orchestrator to deploy the software to systems in your network that are managed.

Task
For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click Menu | Systems | System Tree, then select a group or systems.
3. On the Assigned Client Tasks tab, click Actions, then click New Client Task Assignment.
4. Complete these options, then click Create New Task:
   a. For Product, select McAfee Agent.
   b. For Task Type, select Product Deployment.
5 On the Client Task Catalog page:
   a Type a name for the task.
   b Select Mac as the target platform.
   c In Products and components, select McAfee Endpoint Protection for Mac <version_number> <build_number>, select Install as the action, then click Save.

6 In the Client Task Assignment Builder page:
   a Select the task, then click Next.
   b Schedule the task to run immediately, click Next to view a summary of the task, then click Save.

7 In the System Tree, select the systems or groups where you assigned the task, then click Wake Up Agents.

8 Select Force complete policy and task update, then click OK.

Test the installation

When you have completed the installation, we recommend that you test it to make sure that the software is installed properly and can protect the Mac.

Tasks

• Test the anti-malware protection feature on page 18
   You can test the anti-malware protection feature by accessing the European Institute of Computer Anti-Virus Research (EICAR) standard anti-virus test file.

Test the anti-malware protection feature

You can test the anti-malware protection feature by accessing the European Institute of Computer Anti-Virus Research (EICAR) standard anti-virus test file.

This file is the combined effort by anti-virus vendors to implement one standard that customers can use to validate the anti-virus software.

Task

1 Go to the EICAR website http://www.eicar.org.

2 Click DOWNLOAD ANTI MALWARE TESTFILE, then click DOWNLOAD.

3 Click an anti-malware test file. For example, eicar.com.txt.

For the test to be successful, McAfee VirusScan for Mac displays a message Notification 1 detection(s) found on your system with the relevant details.
Uninstall the software

Remove the software from the standalone Mac and remove the software and its related extensions from the Mac that is managed by ePolicy Orchestrator.

Tasks
- **Uninstall the software from a standalone Mac on page 19**
  You can uninstall the software from a Mac using the command line.
- **Remove the software from a managed Mac on page 19**
  Remove McAfee VirusScan for Mac from the managed Mac and remove the extensions from the ePolicy Orchestrator server.

Uninstall the software from a standalone Mac

You can uninstall the software from a Mac using the command line.

**Before you begin**
You must have administrator rights to uninstall the software.

**Task**
1. Open a Terminal window.
2. Type the following command, then press **return**.
   ```
sudo /usr/local/McAfee/uninstall EPM
   ```
   The uninstallation command is case sensitive.
3. Type the administrator password when prompted.
   When self-protection feature is enabled in **Endpoint Protection for Mac 2.1.0 | General | General Policies**, uninstalling the software using the command line prompts you to type the password provided by the ePolicy Orchestrator administrator.

When the software is uninstalled, the following message appears:

McAfee Endpoint Protection for Mac 2.1.0 has been uninstalled successfully.

When you uninstall the software, the McAfee Agent is not uninstalled from the system. This is because that it might be used by other products. Refer to the product guide of your McAfee Agent version for more information.

Remove the software from a managed Mac

Remove McAfee VirusScan for Mac from the managed Mac and remove the extensions from the ePolicy Orchestrator server.

**Tasks**
- **Remove the software on page 19**
  Create a client task on the ePolicy Orchestrator to remove McAfee VirusScan for Mac from the managed Mac.
- **Remove the software extensions on page 20**
  Remove the McAfee VirusScan for Mac extensions from the ePolicy Orchestrator server.

Remove the software

Create a client task on the ePolicy Orchestrator to remove McAfee VirusScan for Mac from the managed Mac.
Task
For option definitions, click ? in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click Menu | Systems | System Tree, then select a group or systems.

3 Click the Assigned Client Tasks tab, then click New Client Task Assignment.

4 Complete these options, then click Create New Task.
   a For Products, select McAfee Agent.
   b For Task Type, select Product Deployment.

5 On the Client Task Catalog page:
   a Type a name for the task.
   b Select Mac as the target platform.
   c In Products and components, select McAfee Endpoint Protection for Mac 2.1, select Remove as action, then click Save.

6 On the Client Task Assignment Builder page:
   a Select the task, then click Next.
   b Schedule the task to run immediately. Click Next to view a summary of the task, then click Save.

7 In the System Tree, select the systems or groups for which you assigned the task, then click Wake Up Agents.

8 Select Force complete policy and task update, then click OK.

When self-protection feature is enabled in EndPoint Protection for Mac 2.1 | General | General Policies, uninstalling the software using the command line prompts you to type the password provided by the ePolicy Orchestrator administrator.

Remove the software extensions
Remove the McAfee VirusScan for Mac extensions from the ePolicy Orchestrator server.

Task
For option definitions, click ? in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click Menu | Software | Extensions.

3 In the left pane, select the extension and click Remove.

4 Select Force removal, bypassing any checks or errors, then click OK.
Using the software on a standalone Mac

You can use the McAfee VirusScan for Mac console to view the dashboard, events details, the history of all events, quarantined items, and to configure scan schedules.

Contents
- Dashboard
- History of events
- Quarantine malware
- Remove or restore the quarantined item
- Update the anti-malware and DAT files
- Perform a system scan
- Configure custom scan tasks

Dashboard

The dashboard displays the security status of your Mac, malware detection statistics, version details of engine and DAT files, and recent events summary.

To view the dashboard, click the McAfee menulet on the status bar, select McAfee Endpoint Protection for Mac Console, then click Dashboard. The events that are listed in the dashboard are read-only.

Security status

View the security status and the protection features that are enabled or disabled on your Mac.

Use the dashboard to know the status of:

- On-access Scan
- Spyware Scan

Recent events summary

You can view the summary of recent five events in Dashboard.

The events summary includes:

- Status of scan task with number of malware detected from on-access scan and on-demand scan.
- Anti-malware update status with DAT version details.

Recent events displays only the summary of events. To view the complete details of events, navigate to the History page, then double-click the particular event.
History of events

The History page displays all events with details for virus and spyware scanning, anti-malware update, and blocked applications.

To view History, click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Console. Twenty events are listed per page and you can use arrow keys to navigate through pages.

<table>
<thead>
<tr>
<th>To...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>View events</td>
<td>Double-click the event you want to view.</td>
</tr>
<tr>
<td></td>
<td>• Anti-malware Update — Displays the DAT version, engine version, and the status of the update.</td>
</tr>
<tr>
<td></td>
<td>• On-access Scan — Displays the application that accessed the malware, status of detection found, and total number of detections with the details.</td>
</tr>
<tr>
<td></td>
<td>• On-demand Scan — Displays number of files scanned, name and location of infected files, if found, and action taken.</td>
</tr>
<tr>
<td>Sort events</td>
<td>Click the column header to sort events based on title, type, or date and time.</td>
</tr>
<tr>
<td>Remove events</td>
<td>1 Click , type the administrator password, then click OK.</td>
</tr>
<tr>
<td></td>
<td>2 Select the event, then click Delete.</td>
</tr>
<tr>
<td></td>
<td>3 Click OK to remove the events.</td>
</tr>
<tr>
<td></td>
<td><img src="warning.png" alt="Warning: You can't restore the events once you remove them from the list." /></td>
</tr>
<tr>
<td></td>
<td>4 Click to prevent further changes.</td>
</tr>
</tbody>
</table>

Quarantine malware

The quarantine feature isolates dangerous or suspicious malware that could harm your Mac otherwise.

To view the quarantined items, from the status bar, click the McAfee menulet | McAfee Endpoint Protection for Mac Console | Quarantine. The quarantine page displays the original path of items quarantined with date and time of the event. You can either remove or restore the quarantined item.

Remove or restore the quarantined item

The Dashboard displays the list of quarantined items with the path, date, and time. You can restore the quarantined items, only if you are sure that they are non-malicious items, otherwise you can remove them.

Before you begin
You must have administrator rights to remove or restore the quarantined item from the list.

![Warning: Before restoring an item, we recommend that you send it to McAfee Labs for testing. To submit a sample to McAfee Labs, see KB article 68030.](warning.png)
Task
1. Click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Console.
2. On the console dashboard, click Quarantine.
3. Click , type the administrator password, then click OK.
   - To restore, select the quarantined item, click Restore, then click OK to confirm.
   - To remove, select the quarantined item, click Delete, then click OK to confirm.
4. Click to prevent further changes.

Update the anti-malware and DAT files
Always keep anti-malware and DAT files up to date to protect your Mac from the latest threats.

Task
1. Click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Console.
2. On the console dashboard, click Update Now.
3. Click Start Update to initiate the anti-malware update task.

Upon completion, the update summary appears with the engine version, DAT version, update status, and DAT creation date in the Anti-malware Update section. You can view the status and details of anti-malware update event in the History page.

To schedule an automatic update, see Configure anti-malware update schedule.

Perform a system scan
Perform an on-demand scan on specific files, folders, and local or network-mounted volumes immediately.

Task
1. Click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Console.
2. On the console dashboard, click Scan Now.
3. From the What to scan drop-down list, select Start Scan.

Configure custom scan tasks
Schedule and customize scan tasks based on your requirements, to scan specific files, folders, and volumes periodically. You can also modify or remove the existing schedule.
For example, to scan your download folder and music library folder more frequently, you can define a scan schedule for only these two folders.
Tasks

- **Create a scan task on page 24**
  Create scan tasks that automatically run at scheduled periods with the defined parameters.

- **Modify an existing scan task on page 25**
  Modify an existing scan schedule to add or remove locations or change the date and time.

- **Remove an existing scan schedule on page 25**
  Remove the scheduled scan schedule when you no longer need it.

Create a scan task

Create scan tasks that automatically run at scheduled periods with the defined parameters.

Task

1. Click the McAfee menulet 📢 on the status bar, then select **McAfee Endpoint Protection for Mac Console**.
2. On the console dashboard, click **Scan Now**.
3. Click ☐ in the bottom left corner.
4. In the **Scan Name** field, type a name, then click **Create**.
5. From the **What to scan** drop-down list, select the items you want scan. Click + or - to remove the location.
   - **Documents** — Scans the user documents folder.
   - **Desktop** — Scans files and folders in desktop.
   - **Users** — Scans the user directory.
   - **Applications** — Scans the applications folders.
   - **Localhost** — Scans the local host.
   - **Choose** — Allows you to select folder or file location to scan.
6. In the **When to scan** section, select a schedule for the scan task, then click **Schedule Scan**.
   - **Immediately** — Starts a scan task immediately. If you select to scan items immediately, click **Start Scan**.
   - **Once** — Scans the defined locations once at the scheduled date and time.
   - **Daily** — Scans the defined locations every day at the scheduled time. You can define the duration to run the daily scan task or select **No End Date** to run the schedule without any limit.
   - **Weekly** — Scans the defined locations on a scheduled day and time of every week. You can define the duration to run the weekly scan task or select **No End Date** to run the schedule without any limit.
   - **Monthly** — Scans the defined locations on a scheduled date and time of every month. You can define the duration or select **No End Date** to continue the schedule without any limit.
7. When you see a message that the scan task is scheduled, click **OK**.
Modify an existing scan task
Modify an existing scan schedule to add or remove locations or change the date and time.

Task
1. Click the McAfee menulet 🔄 on the status bar, then select McAfee Endpoint Protection for Mac Console.
2. On the console dashboard under Activity, click the schedule you want to modify. The schedule displays the Last Scan Time and Next Scan Schedule.
3. Click Modify Scan, make the needed changes, then click Schedule Scan.

To run the scan schedule immediately, select the scan, make the needed changes, then click Schedule Scan.

Remove an existing scan schedule
Remove the scheduled scan schedule when you no longer need it.

Task
1. Click the McAfee menulet 🔄 on the status bar, then select McAfee Endpoint Protection for Mac Console.
2. On the console dashboard, select an existing scan schedule in the left pane.
3. In the bottom left corner of the console, click 🗑️ to remove the selected item.
Using the software on a standalone Mac
Configure custom scan tasks
Configuring protection preferences on a standalone Mac

Use McAfee VirusScan for Mac preferences to enable or disable anti-malware, anti-spyware, and to configure the protection parameters.

Contents
- General preferences
- Anti-malware
- Configure an update schedule

General preferences
Enable or disable the protection features that you want to run on your Mac.

Configure general preferences
Enable or disable the security features you want to configure for your Mac.

Before you begin
You must have administrator rights to configure these protection preferences.

Task
1. Click the McAfee menulet 📦 on the status bar, then select McAfee Endpoint Protection for Mac Preferences.
2. On the General tab, click 🗝️, type the administrator password, then click OK.
3. Click ON or OFF to enable or disable these features:
   - On-access Scan — Detects malware, whenever a file is read from or written to the hard disk.
   - Spyware Scan — Detects spyware and takes preventive actions.
4. Click ⏰️ to prevent further changes.

McAfee VirusScan for Mac is shipped with the default set of policies. Verify the protection preferences for each component and make sure that it matches your requirements. For more information on setting preferences, see Configure protection preferences.
Anti-malware

Configure anti-malware preferences to define the actions for an on-access scan or on-demand scan, and to exclude specific paths from scanning.

Configure on-access scan preferences

The on-access scan protects your Mac from threats in real time. It scans for malware whenever an item is read from or written to the hard disk, and cleans or quarantines the file according to your configuration.

Task

1. Click the McAfee menulet 🌐 on the status bar, then select McAfee Endpoint Protection for Mac Preferences.

2. On the Anti-malware tab, click 📜, type the administrator password, then click OK.

3. From the Scan files while drop-down list, select one of these options:
   - Read — To scan items when they are read from the hard disk.
   - Write — To scan items when they are written to the hard disk.
   - Read & Write — To scan items when they are read from or written to the hard disk.

4. In Maximum scan time (in seconds), specify the duration allowed to scan each file. You can specify a value between 10 and 999. The default value is 45.

5. From the When a virus is found drop-down list, select one of these options:
   - Clean — To clean the item that contains a virus. Use the If clean fails drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
   - Quarantine — To quarantine the item that contains a virus. Use the If clean fails drop-down list, to select a secondary action (delete the item or send notification)
   - Delete — To delete the item that contains a virus.
   - Notify — To notify you when a virus is detected. No other action is taken.

6. From the When a spyware is found drop-down list, select one of these options:
   - Clean — To clean the item that contains spyware. Use the If clean fails drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
   - Quarantine — To quarantine the item that contains spyware. Use the If clean fails drop-down list, to select a secondary action (delete the item or send notification)
   - Delete — To delete the item that contains spyware.
   - Notify — To notify you when spyware is detected. No other action is taken.

7. From the Also scan drop-down list, select where you want to enable scanning:
   - Archives & Compressed Files
   - Apple Mail Messages
   - Network Volumes

When these options are selected, McAfee VirusScan for Mac will detect the threat. But, the primary and secondary actions may vary depending on the options selected. For more information, see KB article 78277
8 Click to prevent further changes.

**Configure on-demand scan preferences**

Schedule an on-demand scan to run immediately, at a scheduled time, or at regular intervals.

For information on creating a scan task, see [Create a scan task](#).

**Task**

1. Click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Preferences.
2. On the Anti-malware tab, click On-demand Scan.
3. Click , type the administrator password, then click OK to open the On-demand scan page.
4. From the When a virus is found drop-down list, select one of these options:
   - **Clean** — To clean the item that contains a virus. Use the If clean fails drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
   - **Quarantine** — To quarantine the item that contains a virus. Use the If clean fails drop-down list, to select a secondary action (delete the item or send notification)
   - **Delete** — To delete the item that contains a virus.
   - **Notify** — To notify you when a virus is detected. No other action is taken.
5. From the When a spyware is found drop-down, select one of these options:
   - **Clean** — To clean the item that contains spyware. Use the If clean fails drop-down list, to select a secondary action (quarantine the item, delete the item or send notification)
   - **Quarantine** — To quarantine the item that contains spyware. Use the If clean fails drop-down list, to select a secondary action (delete the item or send notification)
   - **Delete** — To delete the item that contains spyware.
   - **Notify** — To notify you when spyware is detected. No other action is taken.
6. From the Also scan drop-down list, select where you want to enable scanning:
   - Archives & Compressed Files
   - Apple Mail Messages
   - Network Volumes

When you run a full scan, by default, all network volumes mounted on your Mac are scanned for threats.

7. Click to prevent further changes.

**Define anti-malware exclusions**

Exclude files and folder paths from an on-access scan or on-demand scan.

**Task**

1. Click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Preferences.
2. Click Anti-malware, then click Exclusions.
3 Click \[\text{login}\], type the administrator password, then click OK.

4 Click \[\text{settings}\] in the bottom left corner of the console.

5 Select the path of the required files and folders, then click Open.

6 Select or deselect the On-access Scan and On-demand Scan options as needed.
   - Double-click an item to change the name or path that appears in the exclusion list.
   - Use regular expressions to exclude items from scanning. For example, to exclude all files in the desktop from scanning, specify the path as /Users/user/Desktop/*.*
   - To remove the item from the exclusions list, select it, then click \[\text{delete}\] in the bottom left corner of the page (or press fn+delete).

   If you deselect the On-access Scan and On-demand Scan options for a path added to the exclusion list, the path is removed from the exclusion list immediately.

7 Click \[\text{done}\] to prevent further changes.

**Best practices for anti-malware preferences**

This section describes the best practices to define the preferences for scheduling on-access scan and on-demand scan.

**On-access scan preferences**

- Always enable On-access-Scan because it checks every file the user accesses, and detects malware before it runs.
- Enable the scan option for the Network Volumes when needed, to scan files copied from or written to any network volumes.
- Always select Quarantine as the secondary action for virus and spyware detections so that you can retrieve the files from the product console later.

**On-demand scan preferences**

- Always enable the scan for Archives & Compressed Files while performing on-demand scan. This is recommended because you may have disabled scanning option for these files.
- Always select Quarantine as the secondary action for virus and spyware detections so that you can retrieve the files from the product console later.

**On-demand scan schedule**

- Schedule an on-demand scan during non-peak hours (for example, during weekends or maintenance period).
- When scheduling an on-demand scan for the first time, schedule a full on-demand scan of your entire hard disk.

**Anti-malware exclusions**

You can add regular expressions that match required patterns to exclude multiple files and folders from being scanned.

Here are some recommended exclusions:
• Microsoft Outlook database files
• Thunderbird database files
• Encrypted files
• Generic plist files such as Info.plist or version.plist for on-access scanning

Here are the regular expressions for some of the recommended exclusions:
• To exclude files with the extension mdb, use .*\ mdb.
• To exclude files with the extension mdb or odc, use .*/ (mdb|odc). 
• To exclude each user’s Entourage/Outlook Database files of different Microsoft Office version, use /Users/.*\ Documents/Microsoft\ \ User\ Data/Office\ \ d+\ Identities/.*Identity/Database.
• To exclude all Info.plist, version.plist under /Applications, use /Applications/.*\ Contents/(version|Info).plist.
• To exclude files with the extensions jar, rar, or war under /private/var/tmp, use /private/var/tmp/.*\..+ar.
• To exclude files under /private/var/tmp starting with a letter and ending with a number, use /private/var/tmp/([A-Z][a-z]).*[0-9]$.

Configure an update schedule

Configure the repository list that needs to be accessed to update the anti-malware, the proxy connection settings, and the anti-malware update schedule.

Tasks
• Configure the repository list on page 31
  Always keep your DAT files and anti-malware up to date to secure your Mac from the latest threats.
• Configure proxy settings on page 32
  Configure Proxy settings if you use proxy servers to connect to the Internet for retrieving packages.
• Configure the anti-malware update schedule on page 32
  Periodic updates of anti-malware secure your Mac from latest threats.

Configure the repository list
Always keep your DAT files and anti-malware up to date to secure your Mac from the latest threats.

The software is shipped with the configuration that allows access to the McAfee FTP server, HTTP server, and the local repository to download the latest DAT files while your Mac is connected to the Internet.

Task
1. Click the McAfee menulet 🗝️ on the status bar, then select McAfee Endpoint Protection for Mac Preferences.
2. Click Update.
3. Click ⌘, type the administrator password, then click OK.
4  In Repository Name list box, on the Repository List tab:
   •  — To add a repository.
   •  — To delete an existing repository.
   •  — To prioritize repositories.

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  On the Schedule tab, schedule the task, then click Apply.

8  Click to prevent further changes.

**Configure proxy settings**
Configure Proxy settings if you use proxy servers to connect to the Internet for retrieving packages.

**Task**
1  Click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Preferences.

2  Click Update, then click the Proxy Settings tab.

3  Click , type the administrator password, then click OK.

4  Select whether to use a proxy.
   •  Do not use a proxy
   •  Configure proxy settings manually

5  Select Use these settings for all proxy types to specify the same IP address and port number for all proxy types.

6  Select FTP or HTTP server, then type the IP address and port number of the selected server.

7  Select Use authentication, then type the user name and password for FTP, HTTP, or a local repository.

8  To bypass a proxy server for specific domains, select the Specify exceptions, then type the proxy server name.

9  Click to prevent further changes.

**Configure the anti-malware update schedule**
Periodic updates of anti-malware secure your Mac from latest threats.

**Task**
1  Click the McAfee menulet on the status bar, then select McAfee Endpoint Protection for Mac Preferences.

2  On the Update tab, click Schedule.

3  Click , type the administrator password, then click OK.
4 Click the drop-down list to select the update frequency, then click **Apply**.
   - **Never** — To never update anti-malware.
   - **Hourly** — To update anti-malware on hourly basis, then select the hours.
   - **Daily** — To update anti-malware daily, then type the time.
   - **Weekly** — To update anti-malware weekly, select weekdays, then type the time.
   - **Monthly** — To update anti-malware monthly, select the day of the month, then type the time.

5 Click ![lock](lock_icon.png) to prevent further changes.
Configuring protection preferences on a standalone Mac
Configure an update schedule
Integrate and manage McAfee VirusScan for Mac using ePolicy Orchestrator management software. McAfee ePolicy Orchestrator provides a scalable platform for centralized policy management and enforcement on your McAfee security products and the systems where they are installed. It also provides comprehensive reporting and product deployment capabilities through a single point of control.

For instructions about setting up and using ePolicy Orchestrator and McAfee Agent, see the product guide for your version of each product.

Contents

- Manage policies
- Create a self-protection policy
- Create an anti-malware policy
- Schedule an anti-malware update
- Schedule an on-demand scan
- Queries and reports

Manage policies

McAfee VirusScan for Mac policies provide options to configure the features, feature administration, and to log details on a managed Mac.

You can find these policies on the Policy Catalog page under Product:

- Endpoint Protection for Mac 2.1.0:Anti-malware
- Endpoint Protection for Mac 2.1.0:General
- McAfee Agent

Configure these policies with your preferences, then assign them to groups of the managed Mac. For generic information about policies, see the product guide for your version of ePolicy Orchestrator.

Tasks

- Create or modify policies on page 35
  You can create and edit policies for a specific group in the System Tree.
- Assign policies on page 36
  When you have created or modified policies, assign them to the systems that are managed by ePolicy Orchestrator.

Create or modify policies

You can create and edit policies for a specific group in the System Tree.
Task
For option definitions, click ? in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.
2 From the Policy Catalog, select a Product and Category.
3 Perform these steps to create or modify a policy.

<table>
<thead>
<tr>
<th>To create a policy</th>
<th>To modify a policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Click New Policy.</td>
<td>1 Click the policy you want to modify.</td>
</tr>
<tr>
<td>2 Type the Policy Name.</td>
<td>2 Modify the settings.</td>
</tr>
<tr>
<td>3 Click OK.</td>
<td></td>
</tr>
<tr>
<td>4 Configure the settings.</td>
<td></td>
</tr>
</tbody>
</table>

4 Click Save.

Assign policies
When you have created or modified policies, assign them to the systems that are managed by ePolicy Orchestrator.

Task
For option definitions, click ? in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.
2 Navigate to System Tree, select a group or systems, then click the Assigned Policies tab.
3 Select a product from the product list, select a policy, then click Edit Assignment.
4 Select the policy to assign, select appropriate inheritance options, then click Save.

Create a self-protection policy
Self-protection allows ePolicy Orchestrator administrators to enable password protection for preferences in the client interface for managed Macs.

Enabling password protection prevents local users from modifying preferences that are defined by the ePolicy Orchestrator administrator, and prevents uninstalling the software on managed Macs. When local users try to modify preferences or try to uninstall the software, the application prompts for the ePolicy Orchestrator password.

Task
For option definitions, click ? in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.
2 From the Policy Catalog, select Endpoint Protection for Mac 2.1.0:General as the product, then select General Policies as the category.
3 Click New Policy, type a name for the policy, then click OK.
4 On the General tab, define these options:
   • Administrator password to unlock client preferences — To enable or disable the password protection.
   • Set password
     • Password — Type the password.
     • Confirm Password — Confirm the password.

   The password must be at least 8 characters.

5 Click Save.

6 In the System Tree, select the systems or groups.

7 In the right pane, click the Group Details tab, then click Wake Up Agents.

8 In Force policy update, select Force complete policy and task update, then click OK.

We recommend that you enable the password protection for preferences to prevent local users from modifying preferences that are defined by the ePolicy Orchestrator administrator, and to prevent local users from uninstalling the software on managed Macs.

---

Create an anti-malware policy

Create anti-malware policies to define parameters for an on-access scan and on-demand scan. You can also create or modify these policies from the System Tree, while assigning policies to selected systems. See the product guide for your version of ePolicy Orchestrator for more information.

Task
For option definitions, click ? in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 From the Policy Catalog, select Endpoint Protection for Mac 2.1.0: Anti-malware as the product, then select Anti-malware as the category.

3 Click New Policy, type a name for the policy, then click OK.

4 On the General tab of the policy page, select these options:
   • General policies controlling overall functioning of Anti-malware — To enable or disable the on-access scan and on-demand scan.
   • Anti-malware update — To disable the local auto update schedule.

5 Click the On-access Scan tab and define these settings:
### In... | Define...
---|---
**On-access Scan policies**
- **Scan contents of Archives and compressed files** — To scan archived and compressed files.
- **Scan Apple Mail Messages** — To scan Apple mail messages.
- **Scan file on Network Volumes** — To scan the files on the mounted network volumes.
- **In Maximum scan time (seconds)**, type a value between 10 and 999.

**Scan files**
- **On Read** — To scan files when you access them to read.
- **On Write** — To scan files when they are written to the hard disk.
- **Read & Write** — To scan files when they are read from or written to the hard disk.

**When a virus is found**
- **Clean** — To clean the item that contains malware.
- **Quarantine** — To isolate the item that contains malware.
- **Delete** — To delete the item that contains malware.
- **Notify** — To notify when malware is detected.

**If the above action fails**
- **Quarantine** — To isolate the item that contains malware.
- **Delete** — To delete the item that contains malware.
- **Notify** — To notify when malware is detected.

**When a spyware is found**
- **Clean** — To clean the item that contains spyware.
- **Quarantine** — To isolate the item that contains spyware.
- **Delete** — To delete the item that contains spyware.
- **Notify** — To notify when spyware is detected.

**If the above action fails**
- **Quarantine** — To isolate the item that contains spyware.
- **Delete** — To delete the item that contains spyware.
- **Notify** — To notify when spyware is detected.

---

6 Click the **On-demand Scan** tab, then define these settings:

<table>
<thead>
<tr>
<th>In...</th>
<th>Define...</th>
</tr>
</thead>
</table>
| **On-demand Scan policies**
- **Scan contents of Archives and compressed files** — To scan archived and compressed files.
- **Scan Apple Mail Messages** — To scan Apple mail messages.
- **Scan file on Network Volumes** — To scan files on mounted network volumes. |

**When a virus is found**
- **Clean** — To clean the item that contains malware.
- **Quarantine** — To isolate the item that contains malware.
- **Delete** — To delete the item that contains malware.
- **Notify** — To notify when malware is detected.

**If the above action fails**
- **Quarantine** — To isolate the item that contains malware.
- **Delete** — To delete the item that contains malware.
- **Notify** — To notify when malware is detected.
Define.. When a spyware is found

- **Clean** — To clean the item that contains spyware.
- **Quarantine** — To isolate the item that contains spyware.
- **Delete** — To delete the item that contains spyware.
- **Notify** — To notify when spyware is detected.

If the above action fails

- **Quarantine** — To isolate the item that contains malware.
- **Delete** — To delete the item that contains malware.
- **Notify** — To notify when malware is detected.

When you run an on-demand scan on managed Macs, events are logged in ePolicy Orchestrator when the scan is started and completed successfully. For more information on events, see KB article 79259.

7 Click the Exclusions tab.
   a In the Exclude specific disks, files and folders text box, type the path you want to exclude from scanning.
      For example, to exclude the file excludethis.docx, which is on the desktop, type /Users/user/Desktop/excludethis.docx.
   b Select On-access-Scan or On-demand Scan as needed to exclude these items.

8 Click Save.

If you disable the On-access Scan and Spyware Scan protection from ePolicy Orchestrator, the security status of the managed Mac still appears that Your Mac is Secured.

## Schedule an anti-malware update

Schedule an update to keep the anti-malware and DAT files up to date.

**Task**

For option definitions, click ? in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click Menu | Systems | System Tree, then select a group or systems.

3 On the Assigned Client Tasks tab, click Actions, then select New Client Task Assignment.
   a For product, select McAfee Agent.
   b For Task Type, select Product Update.
   c Click Create New Task to open the Client Task Catalog.
   d Type a name for the task, select Mac Engine and DAT in Signatures and engines from Package types, then click Save. The task is listed under Task Name.
   e Select the task, then click Next.
4 On the Schedule page, define the schedule for the task.
   a In the System Tree, select the systems or groups where you want to assign the task.
   b Set these values, then click Next.
      • Schedule status
      • Schedule type
      • Effective period
      • Start time
      • Task runs according to
      • Options

5 On the Summary page, click Save.

6 In the right pane, select Group Details, then click Wake Up Agents.

7 In Force policy update, select Force complete policy and task update, then click OK.

---

**Schedule an on-demand scan**

Schedule an on-demand scan to scan the managed systems for threats.

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

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click Menu | Systems | System Tree, then select a group or systems.

3 Click the Assigned Client Tasks tab, then click Actions | New Client Task Assignment.
   a For Product, select Endpoint Protection for Mac 2.1: Anti-malware.
   b For Task Type, select On-Demand Scan Task.
   c Click Create New Task to open the Client Task Catalog page.
   d Type a name for the task, then click Save. The task is listed in Task Name.

4 Select the task, then click Next.

5 Define these parameters, then click Next.
      • Schedule status
      • Schedule type
      • Effective period
      • Start time
      • Task runs according to
      • Options

6 In the Summary page, click Save.

7 In the System Tree, select the systems or groups where you assigned the task.

8 In the right pane, click the Group Details tab, then click Wake Up Agents.

9 In Force policy update, select Force complete policy and task update, then click OK.
Queries and reports

Run predefined queries to generate reports, or modify them to generate custom reports.

<table>
<thead>
<tr>
<th>Query</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPM: Anti-malware Compliance</td>
<td>The current Endpoint Protection for Mac: Anti-malware version compliance.</td>
</tr>
<tr>
<td>EPM: Anti-malware Threats</td>
<td>A line chart of the number of internal virus detections.</td>
</tr>
</tbody>
</table>

Run a query

Run queries to generate reports based on data from McAfee VirusScan for Mac.

**Task**

For option definitions, click ? in the interface.

1. Log on to the ePolicy Orchestrator server as administrator.
2. Click Menu | Reporting | Queries & Reports.
3. From Shared Groups in the Groups pane, select the group.
4. Select a query from the Queries list, then click Actions | Run.
5. Click the item in the results list to view the details.
Troubleshooting

Identify and troubleshoot issues when using McAfee VirusScan for Mac.

Run the repairMSC utility

Use the repairMSC utility to troubleshoot McAfee VirusScan for Mac issues. It generates diagnostic reports, which can be uploaded to the McAfee server for analysis.

Task

1. Open a Terminal window, type the following command, then press return.
   
   `/usr/local/McAfee/repairMSC`

2. Type the administrator password when prompted, then press return.

3. Type `Y` to continue, then press return.

   A consolidated diagnostic report is generated in home directory for issue analysis. A list of issues appears with each category relating to a number from 1 to 8.

4. Type a number that best describes the issue, then press return. The repairMSC runs a repair utility based on the number selected and provides a solution.

5. Type `y` or `n` to confirm whether the issue was fixed, then follow the on-screen instructions.

The report file repairMSC.zip is available in your home directory. (Users/user).

Contact McAfee Support for troubleshooting assistance.
Troubleshooting
Run the repairMSC utility
Index

A
about this guide 5
anti-malware
  best practices 30
  configuring anti-malware 30
  defining exclusions 29
  testing the feature 18
  updating DAT files 23
anti-malware update, ePolicy Orchestrator
  scheduling 39

C
check-in package, ePolicy Orchestrator
  checking in package 17
command-line installation 12
configuration
  general preferences 27
  proxy settings 32
  repository list 31
  scan task 23
  scheduling anti-malware engine update 32
conventions and icons used in this guide 5

D
dashboard
  view events summary 21
  view security status 21
default settings
  anti-malware 14
  general 14
  repository list 14
deployment, ePolicy Orchestrator 17
documentation
  audience for this guide 5
  product-specific, finding 6
  typographical conventions and icons 5

E
EICAR test file 18
events
  viewing details 22
  viewing summary 21

F
features
  product 8
  protection, viewing status 21

H
how the software works 8

I
installation
  command line 12
  extensions 17
  on managed Macs 12
  on standalone Macs 12
  silent 12
  testing 18
  using wizard 12
introduction 7

M
malware
  quarantine 22
  removing quarantined items 22
  restoring quarantined items 22
McAfee ServicePortal, accessing 6

N
need for security 7

O
on-access scan 28
on-demand scan 23
  configuring preferences 29
  creating a task 24
  removing scan task 25
  scheduling for standalone Mac 24
  scheduling from ePolicy Orchestrator 40

P
packages
  checking in 17
  details 12
policies
  assign 36
  create 35
  management 35
  modify 35
policy creation
  anti-malware 37
post installation tasks 15
preferences
  switching 27

Q
quarantine
  malware 22
  removing malware 22
  restoring malware 22
queries, ePolicy Orchestrator 41

R
removal of quarantined item 22
removal of software 19
removal of software extension 20
reports, ePolicy Orchestrator 41

S
scan task
  create 24
  modify 25
ServicePortal, finding product documentation 6
silent installation 12
software
  deployment 16
  repair 43
standalone Mac
  protection preferences 27
system requirements 11

T
Technical Support, finding product information 6