COPYRIGHT
Copyright © 2014 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, 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>Preface</th>
<th>5</th>
</tr>
</thead>
<tbody>
<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>1 Introduction to FIPS</td>
<td>7</td>
</tr>
<tr>
<td>FIPS basics</td>
<td>7</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>7</td>
</tr>
<tr>
<td>The cryptographic boundary</td>
<td>8</td>
</tr>
<tr>
<td>2 Installing and upgrading McAfee ePO in FIPS mode</td>
<td>9</td>
</tr>
<tr>
<td>Installing McAfee ePO in FIPS mode</td>
<td>9</td>
</tr>
<tr>
<td>Upgrade from McAfee ePO 4.6.4</td>
<td>10</td>
</tr>
<tr>
<td>Restoring McAfee ePO server in FIPS mode</td>
<td>10</td>
</tr>
<tr>
<td>Verify that your McAfee ePO server is in FIPS mode</td>
<td>10</td>
</tr>
<tr>
<td>Index</td>
<td>11</td>
</tr>
</tbody>
</table>
Preface

This document provides information you need to install and maintain McAfee® ePolicy Orchestrator® (McAfee ePO™) in FIPS mode.

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.
- **Security officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company's intellectual property.

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

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

**Task**

1. Go to the McAfee ServicePortal at http://support.mcafee.com and click Knowledge Center.

2. Enter a product name, select a version, then click Search to display a list of documents.
McAfee® ePolicy Orchestrator® (McAfee ePO™) provides an operating mode with a higher level of security for environments that require it. This mode (FIPS mode) follows security guidelines detailed in section 140 of the Federal Information Processing Standard (FIPS).

Contents
- FIPS basics
- FIPS mode
- The cryptographic boundary

FIPS basics

The United States Government developed the Federal Information Processing Standards (FIPS) to define procedures, architecture, algorithms, and other techniques used in computer systems. FIPS 140-2 is a government standard for encryption and cryptographic modules where each individual encryption component in the overall solution requires an independent certification.

Federal Information Processing Standard 140-2 specifies requirements for hardware and software products that implement cryptographic functionality. FIPS 140-2 is applicable to "all Federal agencies that use cryptographic-based security systems to protect sensitive [but unclassified] information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104–106." The "-2" in FIPS 140-2 denotes the revision of the standard.

The full FIPS text is available online from the National Institute of Standards and Technology (NIST).

FIPS 140-2 cryptographic modules and certification

McAfee leverages these RSA cryptographic modules to meet the requirements for FIPS-compliance.

Table 1-1  Validated FIPS 140-2 cryptographic modules used by McAfee ePO

<table>
<thead>
<tr>
<th>Cryptographic Module</th>
<th>Certificate number</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA BSAFE Crypto-J JSAFE and JCE (JCM) 6.1</td>
<td>2057</td>
<td><a href="http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2057">http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2057</a></td>
</tr>
</tbody>
</table>

FIPS mode

A McAfee ePO server running in FIPS mode is FIPS-compliant. The decision to run McAfee ePO server in FIPS mode is made at installation and can’t be changed.

In FIPS mode, McAfee ePO:
• Places extra constraints on the types of security methods allowed
• Performs extra tests on startup
• Allows connections only from FIPS-compliant versions of the McAfee Agent.

**Reasons to use McAfee ePO in FIPS mode**

Your organization might need to use McAfee ePO in FIPS mode if you fall into one of these categories:

• You are a US Government organization required to operate FIPS 140-2 compliant cryptographic models per FISMA or other Federal, State, or local regulations.

• Your organization requires the use of standardized and independently evaluated cryptographic modules per Company policy.

**Reasons to not install McAfee ePO in FIPS mode**

Don't use McAfee ePO in FIPS mode if you fall into one of these categories:

• You integrate with legacy systems or products that do not support McAfee ePO in FIPS mode.

• Your organizational polices allow you to choose which products or cryptographic modules to operate in FIPS mode. For example, an organization might elect not to operate McAfee ePO in FIPS mode, and only operate McAfee® Drive Encryption on mobile computers in FIPS mode.

**The cryptographic boundary**

FIPS compliance requires a physical or logical separation between the interfaces by which critical security parameters enter and leave the cryptographic module and all other interfaces. McAfee ePO creates this separation by creating a **boundary** around the cryptographic module. An approved set of interfaces is used to access the modules inside the boundary. No other mechanism to access these modules is allowed or provided when in FIPS mode.

Modules within the boundary perform these processes:

• FIPS-validated security methods performing cryptography, hashing, and related services running within McAfee ePO

• Startup and verification testing required by FIPS

• Extension and executable signature verification

• TLS connection management

• Cryptographic API wrapping utilities

Some older versions of McAfee products use non-FIPS-compliant ways to access McAfee ePO cryptography and hashing services. Because these products violate the cryptographic boundary, they cannot be used in FIPS mode. Check new versions of McAfee products for further information on FIPS compliance as they are released.
Installing and upgrading McAfee ePO in FIPS mode

Follow these instructions to install McAfee ePO in FIPS mode, or to upgrade an existing FIPS mode installation.

There is no supported way to migrate a McAfee ePO server out of FIPS mode. This can only be done with a complete McAfee ePO uninstall and reinstall. Because this process deletes the data in your databases, make sure that your environment requires FIPS mode before proceeding.

Contents
- Installing McAfee ePO in FIPS mode
- Upgrade from McAfee ePO 4.6.4
- Restoring McAfee ePO server in FIPS mode
- Verify that your McAfee ePO server is in FIPS mode

Installing McAfee ePO in FIPS mode

installing McAfee ePO in FIPS mode follows the same basic procedure as outlined in the installation guide. However, FIPS mode installation requires that you run the Setup.exe installer from the command line, adding a command-line option.

Task
1. In a command window, change directories to the folder containing the McAfee ePO installer.
2. Invoke the installer with the command setup.exe ENABLEFIPSMODE=1.
3. Continue with the installation using the instructions in the McAfee ePolicy Orchestrator Installation Guide.

Do not change the default setting for the agent-server secure communication (ASSC) port. Leave it set as enabled on port 443. In FIPS mode, the agents communicate with the McAfee ePO server using this ASSC secure port.
Upgrade from McAfee ePO 4.6.4

Upgrading McAfee ePO with FIPS mode enabled follows the same basic procedure as outlined in the *McAfee ePolicy Orchestrator Installation Guide*. However, FIPS mode upgrades require you to run the Setup.exe installer from the command line, adding a command-line option.

- If your McAfee ePO 4.6.4 server isn't running in FIPS mode, perform a complete reinstallation to change to FIPS mode.
- When you install McAfee ePO in FIPS mode, you can't restore a McAfee ePO database from a previous non-FIPS McAfee ePO server.

**Task**

1. In a command window, change directories to the folder containing the McAfee ePO version 5.1.0 installer.
2. Invoke the installer with the command `setup.exe ENABLEFIPSMODE=1`.
3. Continue with the installation using the instructions in the *McAfee ePolicy Orchestrator Installation Guide*.

Restoring McAfee ePO server in FIPS mode

You can restore a McAfee ePO server in FIPS mode only if the server was previously running in FIPS mode.

You can't restore a McAfee ePO server that wasn't in FIPS mode as a FIPS mode McAfee ePO server. The McAfee ePO software and database must be re-installed as a new instance of McAfee ePO.

The complete McAfee ePO reinstallation is required because all existing signed and encrypted content was signed with non-FIPS mode keys. Also, the database contains content encrypted with non-FIPS mode keys and can't be decrypted with the FIPS mode keys.

Verify that your McAfee ePO server is in FIPS mode

Use the Security Keys page to make sure that your McAfee ePO server is running in FIPS mode.

**Task**

For option definitions, click ? in the interface.

2. Look at the Server.ini value.
   - If the Server.ini value is FipsMode=1, your McAfee ePO server is in FIPS mode.
# Index

**A**
- about this guide 5

**C**
- command-line option 9, 10
- conventions and icons used in this guide 5
- cryptographic boundary
  - definition 8
  - how products violate it 8

**D**
- documentation
  - audience for this guide 5
  - product-specific, finding 6
  - typographical conventions and icons 5

**F**
- Federal Information Processing Standard, See FIPS
- FIPS
  - about 7
  - compliance 7, 8
  - online availability 7
- FIPS mode 7
  - installing McAfee ePO in 9
  - reasons to not install 7
  - reasons to use 7
  - restoring McAfee ePO in 10

**I**
- installation
  - command-line option 9
  - FIPS mode 9

**M**
- McAfee ServicePortal, accessing 6

**R**
- restoring 10

**S**
- server.ini file 10
- ServicePortal, finding product documentation 6

**T**
- technical support, finding product information 6

**U**
- upgrades
  - command-line option 10
  - FIPS mode 10

---

FIPS mode 7 (continued)
- upgrading McAfee ePO in 9, 10
- verifying 10