User Guide

McAfee ePolicy Orchestrator 5.3.0
Software
FIPS Mode
# Contents

**Preface**  
About this guide .................................. 5  
Audience .................................. 5  
Conventions .................................. 5  
Find product documentation .............................. 6  

1 Introduction to FIPS  
FIPS basics .................................... 7  
FIPS mode ..................................... 8  
The cryptographic boundary ............................. 8  

2 Installing and upgrading McAfee ePO in FIPS mode  
Installing McAfee ePO in FIPS mode ....................... 9  
Upgrade from an earlier FIPS-compliant McAfee ePO server ........................................ 10  
Restoring McAfee ePO server in FIPS mode .................... 10  
Verify that your McAfee ePO server is in FIPS mode .................... 10  

A McAfee ePO operating modes  

Index  


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.
Introduction to FIPS

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>
</table>

This module is used only for TLS communication between McAfee ePO and the McAfee Agent.
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 an earlier FIPS-compliant McAfee ePO server
- 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 an earlier FIPS-compliant McAfee ePO server

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.

**Before you begin**

If your existing McAfee ePO 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 new 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.

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

View the server.ini file make sure that your McAfee ePO server is running in FIPS mode.

**Task**

1. Use a text editor to open the server.ini file.
   The server.ini file is located in your McAfee ePO installation directory: `<epoinstalldirectory>\DB\server.ini`.
2. Look for the FipsMode value.
   This value indicates the server operating mode:
   - FipsMode=0 — The server is in Mixed (normal) mode. Repeat the installation or upgrade process to put your server in FIPS mode.
   - FipsMode=1 — The server is in FIPS mode.
   - FipsMode=2 — The server is in Transition mode. After your agent-server communication security keys are updated, the server runs in FIPS mode.
McAfee ePO operating modes

Depending on your environment and installation choices, McAfee ePO operates in one of three modes: FIPS, Transition, or Mixed.

The mode that a McAfee ePO server runs in is determined during installation or upgrade and can't be changed.

FIPS mode

A McAfee ePO server runs in FIPS mode after a clean installation with FIPS mode enabled.

In FIPS mode, McAfee ePO:

• Places extra constraints on the types of security methods allowed
• Performs additional tests on startup
• Allows connections only from a FIPS-compliant version of the McAfee Agent

Transition mode

After upgrading from a previous version of McAfee ePO software that uses an external FIPS-validated cryptographic module (for example, McAfee ePO 4.5.7), the software runs in Transition mode. McAfee ePO continues running in Transition mode until all previous agent-server communication key material has been replaced. After this material has been replaced, the software runs in FIPS mode.

In Transition mode, McAfee ePO generates only 3,072-bit SHA-256 certificates and 2,048-bit SHA-256 agent-server communication keys. McAfee Agent versions earlier than 4.6.0 and existing McAfee products that were connecting to the McAfee ePO server before the upgrade continue to function. New McAfee Agent products that understand the larger key sizes use the larger, more secure FIPS-compliant certificate keys.

After all deprecated keys are removed from the database, the McAfee ePO server runs in FIPS mode. However, existing SSL certificates continue to be lower strength than the certificates included in the most recent FIPS recommendations.

In Transition mode, McAfee ePO still follows the constraints and tests listed for FIPS mode, but relaxes the version restrictions on agents and managed products.

Mixed mode

This mode is a standard McAfee ePO installation not running in FIPS mode.

In Mixed mode, McAfee ePO does not follow the constraints and tests described for FIPS mode, and is not compliant with FIPS levels of security.

Your managed systems are still secure, but the certificates and Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are different.
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 8
  online availability 7
FIPS mode 7, 8
definition 11
installing McAfee ePO in 9
reasons to not install 8
reasons to use 8
restoring McAfee ePO in 10
upgrading McAfee ePO in 9, 10
verifying 10

I
installation
  command-line option 9
  installation (continued)
    FIPS mode 9

M
McAfee ServicePortal, accessing 6
Mixed mode
definition 11

O
operating modes 11

R
restoring 10

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

T
technical support, finding product information 6
Transition mode
definition 11

U
upgrades
  command-line option 10
  FIPS mode 10