User Guide

FIPS Mode

For use with ePolicy Orchestrator 4.6.x Software
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preface</strong></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 to FIPS</strong></td>
<td>7</td>
</tr>
<tr>
<td>FIPS basics</td>
<td>7</td>
</tr>
<tr>
<td>Compliance levels</td>
<td>10</td>
</tr>
<tr>
<td>FIPS operating modes</td>
<td>10</td>
</tr>
<tr>
<td>Implementation basics</td>
<td>11</td>
</tr>
<tr>
<td>Software requirements</td>
<td>12</td>
</tr>
<tr>
<td><strong>2 FIPS mode installation of ePolicy Orchestrator</strong></td>
<td>13</td>
</tr>
<tr>
<td>Installing ePolicy Orchestrator in FIPS mode</td>
<td>13</td>
</tr>
<tr>
<td>Upgrading to FIPS mode from a prior version of ePolicy Orchestrator software</td>
<td>14</td>
</tr>
<tr>
<td>Upgrade from ePolicy Orchestrator 4.5</td>
<td>15</td>
</tr>
<tr>
<td>Upgrade ePolicy Orchestrator 4.5 with EEC installed</td>
<td>15</td>
</tr>
<tr>
<td>ePolicy Orchestrator 4.0 and SSL Certificates</td>
<td>15</td>
</tr>
<tr>
<td>Upgrading ePolicy Orchestrator 4.0 servers to FIPS mode</td>
<td>16</td>
</tr>
<tr>
<td>Installing the McAfee Agent</td>
<td>16</td>
</tr>
<tr>
<td>Restoring ePolicy Orchestrator server in FIPS mode</td>
<td>16</td>
</tr>
<tr>
<td><strong>3 Maintaining a FIPS-compliant environment</strong></td>
<td>17</td>
</tr>
<tr>
<td>How to keep ePolicy Orchestrator FIPS compliant</td>
<td>17</td>
</tr>
<tr>
<td>How to distinguish between FIPS modes</td>
<td>19</td>
</tr>
<tr>
<td>FIPS and the certificate hierarchy</td>
<td>19</td>
</tr>
<tr>
<td>FIPS mode behavior at startup</td>
<td>20</td>
</tr>
<tr>
<td>Secure Socket communication in FIPS mode</td>
<td>21</td>
</tr>
<tr>
<td>McAfee products that support FIPS mode</td>
<td>22</td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>23</td>
</tr>
</tbody>
</table>
Preface

This document provides information you need to install and maintain the enhanced security mode of your McAfee product.

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

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 Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Select a product, then select a version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introduction to FIPS

McAfee ePolicy Orchestrator version 4.6.0 (build 1039) through, and including, version 4.6.4 and the McAfee Agent version 4.6.0 (build 1694 or later) provide an operating mode with a higher level of security for environments that require it. This mode follows security guidelines detailed in section 140 of the Federal Information Processing Standard.

> ePolicy Orchestrator version 5.0 has not been FIPS certified.

Contents
- FIPS basics
- Compliance levels
- FIPS operating modes
- Implementation basics
- Software requirements

FIPS basics

The Federal Information Processing Standards (FIPS) were developed by the United States Government to define procedures, architecture, algorithms, and other techniques used in computer systems.

FIPS is a government standard for encryption and cryptographic modules where each individual encryption component in the overall solution requires an independent certification. In the context of ePolicy Orchestrator, we are concerned with Section 140 of these standards.

> Throughout this document, FIPS refers to FIPS 140-2.

Federal Information Processing Standard 140 (FIPS 140-2, or "the Standard") specifies requirements for hardware and software products that implement cryptographic functionality. FIPS 140 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.

> FIPS certification is a formal government recognition for the effectiveness of a level of security, not necessarily an indicator of greater security.

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

Reasons to use ePolicy Orchestrator in FIPS mode

Your organization might need to use ePolicy Orchestrator in FIPS mode if:
• You are a Federal Government department or contractor. FIPS 140-1 became a mandatory standard for the protection of sensitive data when the Secretary of Commerce signed the standard on January 11, 1994. FIPS 140-2 supersedes FIPS 140-1 and the standard was signed on May 25, 2001.

• You are legally required to use ePolicy Orchestrator to manage only FIPS-validated products.

**Reasons to not enable ePolicy Orchestrator in FIPS mode**

You don't need to use ePolicy Orchestrator in FIPS mode if:

• You want to increase your security. The security of the ePO system is similar whether running in FIPS or non-FIPS modes. FIPS mode operation only ensures adherence to the documented process and APIs evaluated during the FIPS validation process.

• If you are a private sector non-government organization that does business with the government, you may be required to secure systems, like laptops, that might be brought onto government premises using FIPS-validated encryption keys. This figure shows that it might be sufficient to install a product like Endpoint Encryption for PC (EEPC) in FIPS mode, while the overall security solution (including ePolicy Orchestrator and the McAfee Agent) does not require FIPS validation. McAfee recommends you verify the requirements with your auditor and government customer.

**FIPS Section 140-2**

This portion of the standard describes requirements for cryptographic modules that could include both software and hardware components. The standard states that systems complying with higher levels of the standard are more secure than systems that do not. Version 2 of the standard, officially designated FIPS 140-2, was issued on May 25, 2001, and is the version against which the ePolicy Orchestrator software is certified.
FIPS encryption changes for 2011

In January 2011, NIST released Special Publication (SP) 800-131A. This publication specifies stronger encryption strength recommendations than were originally provided in FIPS 140-1 documentation. As a result, the ePolicy Orchestrator software adheres to the updated specifications for selecting algorithms and key sizes.

When upgrading your McAfee ePO software from a previous version, the software continues to use some pre-existing key material (keys and certificates) that are considered to be "legacy" or "deprecated" by the requirements specified in SP 800-131A. All new key material generated after installation of ePolicy Orchestrator version 4.6.x complies with the updated security strength requirements.

FIPS 140-2 compliance levels

FIPS defines four levels of compliance.

Any terms presented in quotation marks are taken from the standard itself and defined there.

### Table 1-1  FIPS compliance levels

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>The lowest level of security. All components are &quot;production-grade&quot; and obvious security holes are absent.</td>
</tr>
<tr>
<td>Level 2</td>
<td>Level 1 plus requirements for role-based authentication and evidence of physical tampering.</td>
</tr>
<tr>
<td>Level 3</td>
<td>Level 2 plus requirements for physical tamper-resistance and identity-based authentication. Additionally, a module should be created with either a physical or logical separation between the interfaces by which &quot;critical security parameters&quot; enter and leave this module and its other interfaces.</td>
</tr>
<tr>
<td>Level 4</td>
<td>Level 3 plus requirements for robustness against environmental attacks. ePolicy Orchestrator does not attempt this level of compliance.</td>
</tr>
</tbody>
</table>

McAfee FIPS Validation

To support these Federal agencies, McAfee maintains an active and strategic program for validating products to meet the assurance needs of end users. As such, these products have received FIPS 140-2 validation.

<table>
<thead>
<tr>
<th>Solution</th>
<th>Validation Link</th>
</tr>
</thead>
</table>

The first steps in pursuing a FIPS 140-2 validation are to define a cryptographic boundary and an overall level of validation. The cryptographic boundary for each product is defined as a narrow set of cryptographic functions, and each module received an overall Level 1 rating with Level 2 for Roles, Services, and Authentication, and Level 3 for Design Assurance.

ePolicy Orchestrator 4.6.1 (and later) and McAfee Agent 4.6 (and later) can be installed either in non-FIPS mode (default) or FIPS mode. The difference between FIPS and default ePolicy Orchestrator and McAfee Agent encryption is that FIPS mode encryption implements algorithms and internal self-tests that are required by the FIPS 140-2 standard.

Both modes of operation are secure. Each cryptographic module protects respective internal data and secures the communication between the McAfee Agent and ePolicy Orchestrator.
Some McAfee products that integrate with ePolicy Orchestrator provide FIPS-validated encryption components as well as the default encryption method that is already in place. Each component may be installed independently from the mode in which other products are installed. The installation mode depends on the use case that the administrator addresses. For commercial (non-government) customers, there are often no requirements that you install the end-to-end solution in FIPS mode. For example, you can install Endpoint Encryption for PC (EEPC) in FIPS mode with a default (non-FIPS) installation of ePolicy Orchestrator and McAfee Agent.

### How FIPS 140-2 applies to ePolicy Orchestrator and the McAfee Agent

To achieve FIPS 140-2 validation, McAfee made significant security enhancements to ePolicy Orchestrator and McAfee Agent that apply to both the default and FIPS modes. These enhancements include using the latest approved and recommended cryptographic algorithms and key lengths as well as isolating cryptographic functions within specific sub-systems. A small set of changes that apply only in FIPS mode include replacing certain APIs to follow the architecture required to achieve FIPS validation.

The encryption used by running ePolicy Orchestrator in default and FIPS mode:
- Protects certain data stored in, and the communications to, the SQL database
- Secures the communications between the server and the McAfee Agent
- Secures the communications between the server, browser, and other types of agents, for example Rogue System Detection (RSD) and Network Access Control (NAC) sensors.

### Compliance levels

ePolicy Orchestrator complies with FIPS at different levels in different areas of the product. When running in FIPS mode, ePolicy Orchestrator 4.6 provides the following levels of FIPS compliance.

<table>
<thead>
<tr>
<th>Product area</th>
<th>FIPS compliance level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall level of security for ePolicy Orchestrator 4.6</td>
<td>Level 1</td>
</tr>
<tr>
<td>Roles, services, and authentication</td>
<td>Level 2</td>
</tr>
<tr>
<td>Design assurance</td>
<td>Level 3</td>
</tr>
</tbody>
</table>

When ePolicy Orchestrator is running in Transition or Mixed mode (described in *FIPS operating modes*), McAfee makes no claim to a specific FIPS compliance level.

### FIPS operating modes

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

The mode that an ePolicy Orchestrator server runs in is decided during installation or upgrade and can't be changed.

#### FIPS mode

This is the mode that an ePolicy Orchestrator server runs in after a clean installation with FIPS mode enabled. In this mode, ePolicy Orchestrator is fully compliant with all targeted FIPS security levels.

In FIPS mode, ePolicy Orchestrator:
• Places extra constraints on the types of security methods allowed
• Performs additional tests on startup
• Allows connections only from McAfee Agent version 4.6 and later

**Transition mode**

When upgrading to version 4.6.x from a previous version of ePolicy Orchestrator software that uses an external FIPS validated cryptographic module (For example, versions 4.0 and 4.5), the software runs in Transition mode. It 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, ePolicy Orchestrator generates only 3,072 bit, SHA-256 certificates and 2,048 bit SHA-256 agent-server communication keys. Agent versions prior to 4.6 and existing McAfee products that were connecting to the server before the upgrade continue to function, and new McAfee products that understand the larger key sizes will use the larger, more secure FIPS-compliant certificates keys recommended for use in 2011.

After all deprecated keys have been removed from the database, the ePolicy Orchestrator server runs in FIPS mode, with the caveat that existing SSL certificates continue to be lower strength than those included in the 2011 recommendations.

In Transition mode, ePolicy Orchestrator still follows the constraints and tests listed for FIPS mode, but relaxes the restrictions on agent and McAfee managed product versions.

**Mixed mode**

This is a standard ePolicy Orchestrator installation not running in FIPS mode. ePolicy Orchestrator versions 4.5 and earlier can operate in this mode only.

In Mixed mode, ePolicy Orchestrator 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 very secure, but the certificates and Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are different.

**Implementation basics**

It is easier to keep an ePolicy Orchestrator system FIPS compliant if you understand the basics of the FIPS implementation.

To understand the basics of FIPS implementation see *Maintaining a FIPS-compliant environment* for details about FIPS compliance, modes, certificate hierarchy, and more.

One of the requirements for FIPS compliance is a physical or logical separation between the interfaces by which critical security parameters enter and leave the cryptographic module and all other interfaces. ePolicy Orchestrator 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 or Transition mode.

**Inside the cryptographic boundary**

Operations performed by modules within the boundary include:
• FIPS-validated security methods performing cryptography, hashing, and related services running within ePolicy Orchestrator
• Startup and verification testing required by FIPS
• Extension and executable signature verification
• TLS connection management
• Cryptographic API wrapping utilities

Outside the cryptographic boundary
Some portions of ePolicy Orchestrator do not need to interact with modules inside the boundary. These areas do not need cryptography or hashing services, and as a result function identically regardless of FIPS mode.

Some older versions of McAfee products use non-FIPS-compliant ways to access ePolicy Orchestrator 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.

Software requirements
FIPS compliance requires that your operating system and browser meet specific requirements for versions and settings.

Not all versions of browsers or operating systems can handle the cryptographic demands FIPS requires. As a result, some operating systems and browsers ePolicy Orchestrator normally supports are not supported in FIPS or Transition mode.

Supported operating systems
To run in FIPS or Transition mode, ePolicy Orchestrator must be installed on one of the following operating systems:
• Windows Server 2008 SP2 or later (32- or 64-bit)
• Windows Server 2008 R2 (64-bit)
• Windows 2008 Small Business Server

Supported browsers
The following browsers are required to connect to an ePolicy Orchestrator server running in FIPS mode:
• Internet Explorer 7.0 or 8.0, running on Windows Vista, Windows 7, or Windows Server 2008.

When using Internet Explorer on a Windows operating system older than these, you can only connect to ePolicy Orchestrator servers running in Mixed or Transition mode due to the security strength of the SSL certificate.
• Firefox 3.5 or 3.6
FIPS mode installation of ePolicy Orchestrator

As FIPS mode cannot be changed without a full re-installation, ensure your environment requires FIPS mode before proceeding.

There is no supported way to migrate an ePolicy Orchestrator server out of FIPS mode. This can only be done with a complete ePolicy Orchestrator uninstall and reinstall. Because this process will destroy any data in your databases, you should be sure about your decision to move to FIPS mode.

Contents

- Installing ePolicy Orchestrator in FIPS mode
- Upgrading to FIPS mode from a prior version of ePolicy Orchestrator software
- Installing the McAfee Agent
- Restoring ePolicy Orchestrator server in FIPS mode

Installing ePolicy Orchestrator in FIPS mode

Installing ePolicy Orchestrator in FIPS mode requires a command-line option.

In general, installing ePolicy Orchestrator in FIPS mode follows the same basic procedure as outlined in the ePolicy Orchestrator 4.6 Install 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 ePolicy Orchestrator installer.
2. Invoke the installer with the command `setup.exe ENABLEFIPSMODE=1`.
3. Continue with the installation using the instructions in the ePolicy Orchestrator 4.6 Install Guide.

Do not change the default setting for the Agent-to-server communication (ASC) secure port. It should be set as enabled on port 443. In FIPS mode the McAfee Agents communicate with the ePolicy Orchestrator server using this ASC secure port.
Upgrading to FIPS mode from a prior version of ePolicy Orchestrator software

If you are upgrading to ePolicy Orchestrator 4.6.x running in FIPS mode, you must follow the supported upgrade path. To upgrade to ePolicy Orchestrator version 4.6.x from version 4.0, you must first upgrade your server to version 4.5. Upgrades of ePolicy Orchestrator from version 4.0 directly to version 4.6.x are not supported.

Tasks

- **Upgrade from ePolicy Orchestrator 4.5 on page 15**
  Upgrading an ePolicy Orchestrator 4.5 server then to 4.6.x with FIPS mode enabled puts your server into Transition mode.

- **Upgrade ePolicy Orchestrator 4.5 with EEC installed on page 15**
  If you have an ePolicy Orchestrator 4.5 server with Endpoint Encryption for PC (EEC) deployed, then upgrade to 4.6.x with FIPS mode, when you update the McAfee Agent all certification standards are updated as well.

- **Upgrading ePolicy Orchestrator 4.0 servers to FIPS mode on page 16**
  Extra steps are required if you are upgrading an ePolicy Orchestrator 4.0 server to 4.6 with FIPS mode enabled to manage SSL connectivity.
Upgrade from ePolicy Orchestrator 4.5

Upgrading an ePolicy Orchestrator 4.5 server then to 4.6.x with FIPS mode enabled puts your server into Transition mode.

In general, upgrading ePolicy Orchestrator with FIPS mode enabled follows the same basic procedure as outlined in the *ePolicy Orchestrator 4.6 Install Guide*. However, FIPS mode upgrades require you to run the `Setup.exe` installer from the command line adding a command-line option.

![Warning: Cannot restore ePolicy Orchestrator database from non-FIPS server.]

When you install ePolicy Orchestrator in FIPS mode you cannot restore an ePolicy Orchestrator database from a previous non-FIPS ePolicy Orchestrator server.

**Task**

1. In a command window, change directories to the folder containing the ePolicy Orchestrator version 4.6.x installer.
2. Invoke the installer with the command `setup.exe ENABLEFIPSMODE=1`.
3. Continue with the installation using the instructions in the *ePolicy Orchestrator 4.6 Install Guide*.

Upgrade ePolicy Orchestrator 4.5 with EEC installed

If you have an ePolicy Orchestrator 4.5 server with Endpoint Encryption for PC (EEC) deployed, then upgrade to 4.6.x with FIPS mode, when you update the McAfee Agent all certification standards are updated as well.

Previous ePolicy Orchestrator versions used a FIPS approved library for cryptography. Any product configured in FIPS or non-FIPS mode continue to operate in that mode after you update to ePolicy Orchestrator version 4.6.x. If you update the ePolicy Orchestrator server to FIPS mode and deploy the new McAfee Agent the certification standard is also updated.

These steps can update your ePolicy Orchestrator 4.5 server with EEC product deployed to full FIPS mode certification after upgrade.

**Task**

1. In a command window, change directories to the folder containing the ePolicy Orchestrator version 4.6.x installer.
2. Invoke the installer with the command `setup.exe ENABLEFIPSMODE=1`.
3. Continue with the installation using the instructions in the *ePolicy Orchestrator 4.6 Install Guide*.
4. After the upgrade is complete, deploy the new McAfee Agent to all managed systems.

Now all managed system with EEC product deployed and the FIPS compliant McAfee Agent are all up to FIPS certification standard.

ePolicy Orchestrator 4.0 and SSL Certificates

ePolicy Orchestrator 4.0 did not support SSL connections. They were introduced with ePolicy Orchestrator 4.5.

A normal upgrade to ePolicy Orchestrator 4.6 activates SSL connections, and creates an SSL certificate hierarchy. Normally this is not an issue, as the standard ePolicy Orchestrator SSL certificate strength is understood by McAfee Agent versions prior to 4.6.

However, if you upgrade directly from ePolicy Orchestrator software version 4.0 to version 4.6 with FIPS mode enabled, McAfee Agent versions prior to 4.6 cannot make SSL connections to that newly upgraded server because the SSL certificate hierarchy was created with stronger encryption than the older agent versions can use. Because of this, the ePolicy Orchestrator installer deactivates the SSL port when upgrading an ePolicy Orchestrator 4.0 server to 4.6 with FIPS mode enabled.
Upgrading ePolicy Orchestrator 4.0 servers to FIPS mode

Extra steps are required if you are upgrading an ePolicy Orchestrator 4.0 server to 4.6 with FIPS mode enabled to manage SSL connectivity.

Versions of ePolicy Orchestrator prior to 4.5 did not support SSL connections. Since SSL connections are required for FIPS compliance, follow this procedure to activate SSL connectivity.

Task

1. Upgrade your 4.0 ePolicy Orchestrator server to version 4.5 of the software.

2. Upgrade your server normally as described in Upgrading from ePolicy Orchestrator 4.5.

When you install ePolicy Orchestrator in FIPS mode you cannot restore an ePolicy Orchestrator database from a previous non-FIPS ePolicy Orchestrator server.

3. Upgrade all agents communicating with the newly upgraded server to McAfee Agent version 4.6.

4. Activate the SSL port on your server.

5. Upgrade to ePolicy Orchestrator server version 4.5 using the FIPS command line option. See Upgrade from ePolicy Orchestrator 4.5 for command line details.

Installing the McAfee Agent

You must follow specific steps when installing the McAfee Agent on an ePolicy Orchestrator server running in FIPS mode

Installation of the 4.6.0 McAfee Agent requires that two content packages be checked into your master repository; the McAfee Agent 4.6 package, and the agent key updater package (automatically checked in). Once these packages have been checked in, installation is completed by deploying the agent to your client systems.

To deploy the 4.6 agent, follow the normal agent deployment scenarios included in the McAfee Agent 4.6.0 Product Guide.

When the 4.6 agent is installed on a system where a prior version was installed, the system first connects to the server using the existing security keys provided by the previous agent. After the first communication with the server, the agent receives a request from the server to upgrade to the stronger 2048-bit or 3072-bit RSA key size and switches to FIPS mode.

Restoring ePolicy Orchestrator server in FIPS mode

When restoring an ePolicy Orchestrator server, running in FIPS mode, that server must have been previously running in FIPS mode. You can't restore a non-FIPS mode ePolicy Orchestrator server as a FIPS mode server.

If you have an ePolicy Orchestrator server running in non-FIPS mode you can't use any of the previous server or database folders, or the database, and convert the server to a FIPS mode ePolicy Orchestrator server. The entire ePolicy Orchestrator software and database must be completely installed as a new instance of ePolicy Orchestrator.

The complete ePolicy Orchestrator reinstallation is required because all existing signed and encrypted content was signed with non-FIPS mode keys. Also, the database contains encrypted content encrypted with non-FIPS mode keys and can't be decrypted with the FIPS mode keys.
Maintaining a FIPS-compliant environment

After installing ePolicy Orchestrator to create a FIPS-compliant environment, you must keep your server compliant.

Contents
- How to keep ePolicy Orchestrator FIPS compliant
- How to distinguish between FIPS modes
- FIPS and the certificate hierarchy
- FIPS mode behavior at startup
- Secure Socket communication in FIPS mode
- McAfee products that support FIPS mode

How to keep ePolicy Orchestrator FIPS compliant
Keeping an ePolicy Orchestrator server FIPS-compliant requires following certain conventions.

Managing non-FIPS-compliant software

ePolicy Orchestrator allows you to check in any properly packaged software to the master repository. This behavior does not change when operating in FIPS mode. As a result, you could have non-FIPS-compliant software in any branch of your master repositories. This might include older versions of McAfee software, or non-McAfee software. But, to maintain a FIPS-compliant operating environment, that non-FIPS-compliant software should not be deployed to managed systems.

ePolicy Orchestrator servers running in FIPS mode could deploy non-compliant agents if they are checked in to the repository and the server is configured to do so. If this occurs, these agents can no longer communicate with an ePolicy Orchestrator server running in FIPS mode.

Some government ePolicy Orchestrator servers must be totally FIPS compliant, but commercial—non-government—ePolicy Orchestrator servers who connect to government networks are not required to install an end-to-end solution in FIPS mode. These users might have an ePolicy Orchestrator server configured similar to this figure.
In this figure, the systems in:

- The red box are totally FIPS compliant
- The blue box are not FIPS compliant, but they can be managed by the ePolicy Orchestrator server in FIPS mode
- No box can’t connect to the FIPS mode ePolicy Orchestrator server because McAfee Agent version 4.5 is not FIPS compliant

To keep from deploying non-FIPS-compliant packages, McAfee recommends:

- Do not check in non-FIPS-compliant packages to the master repository, including McAfee Agent version 4.5 and earlier.
- If you must check in non-FIPS-compliant packages, however, keep non-FIPS-compliant packages in the Previous or Evaluation branches of the master repository carefully manage which branch of the master repository your product update tasks use.

**Agents and Agent Handlers**

McAfee Agent 4.6 runs in FIPS mode when connecting to an ePolicy Orchestrator 4.6 server running in FIPS mode. If the server is running in Transition mode, McAfee Agent versions 4.0 and 4.5 use the lower strength 1,024-bit key, whereas version 4.6 McAfee Agents will switch into FIPS mode and use the higher strength keys.

Deploying Agent Handlers from ePolicy Orchestrator 4.6 is seamless. The Agent Handler installer knows what FIPS mode the server is operating in, and installs the handler accordingly.

**Extensions that cause a FIPS mode server to fail at startup**

The ePolicy Orchestrator extensions that integrate with the BMC Remedy Action Request System and Hewlett-Packard OpenView ServiceDesk ticketing servers are not compatible with an ePolicy Orchestrator server running in FIPS mode. These extensions lack appropriate signature files and cause the server to fail at startup.
How to distinguish between FIPS modes

The only page in ePolicy Orchestrator that indicates a server’s FIPS mode is the Security Keys page. Information about a server’s FIPS mode is also stored in the Server.ini and security files.

Table 3-1   Ways to determine FIPS operating mode

<table>
<thead>
<tr>
<th>Mode</th>
<th>Indicators</th>
</tr>
</thead>
</table>
| FIPS mode     | • Server settings Security Keys page indicates FIPS 140-2 mode  
                • Server.ini: FipsMode=1  
                • The following entries in the `<epo_install_directory>/jre/lib/security/java.security` file:  
                  • orion.fips140.mode=true  
                  • com.rsa.cryptoj.jce.fips140initialmode=FIPS140_MODE |
| Transition mode| • Server settings Security Keys page indicates non-compliant security keys  
                 • Server.ini: FipsMode=2  
                 • The following entries in the `<epo_install_directory>/jre/lib/security/java.security` file:  
                   • orion.fips140.mode=true  
                   • com.rsa.cryptoj.jce.fips140initialmode=FIPS140_MODE |
| Mixed mode    | • No compliance indicators in the Server settings Security Keys page  
                 • Server.ini: FipsMode=0  
                 • The following entries in the `<epo_install_directory>/jre/lib/security/java.security` file:  
                   • orion.fips140.mode=false  
                   • com.rsa.cryptoj.jce.fips140initialmode=NON_FIPS140_MODE |

FIPS and the certificate hierarchy

ePolicy Orchestrator maintains a certificate hierarchy to complete SSL connections. The strength and encryption of these certificates depend on FIPS mode.

One of the benefits of FIPS mode is increased security around connections to the ePolicy Orchestrator server. SSL connections are required and use more secure certificates. The strength and encryption of the certificates used by your server depend on the server’s mode and installation type.

Certificates are generated in one of these security strengths:

- 1,024-bit key, SHA1 digest
- 2,048-bit key, SHA1 digest
- 3,072-bit key, SHA256 digest

There are three categories of certificates used by ePolicy Orchestrator:
• ePolicy Orchestrator certificates (SSL and non-user-interface connections)
• Agent Handler certificates
• Rogue System Detection (RSD) sensor certificates

This table indicates the certificate strength and encryption type stored in the ePolicy Orchestrator database depending on your installation type.

<table>
<thead>
<tr>
<th>Installation type</th>
<th>Orion certificates</th>
<th>Agent Handler certificates</th>
<th>RSD Sensor certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>New installation, FIPS mode</td>
<td>3072/SHA256</td>
<td>3072/SHA256</td>
<td>3072/SHA256</td>
</tr>
<tr>
<td>New installation, Mixed mode</td>
<td>2048/SHA1</td>
<td>2048/SHA1</td>
<td>2048/SHA1</td>
</tr>
<tr>
<td>Upgrade from 4.5, Mixed mode</td>
<td>1024/SHA1</td>
<td>Pre-existing: 1024/SHA1</td>
<td>Pre-existing: 1024/SHA1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New: 2048/SHA1</td>
<td></td>
</tr>
<tr>
<td>Upgrade from 4.5, Transition Mode</td>
<td>1024/SHA1</td>
<td>Pre-existing: 1024/SHA1</td>
<td>Pre-existing: 1024/SHA1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New: 3072/SHA256</td>
<td></td>
</tr>
</tbody>
</table>

Other products that generate child certificates follow a similar pattern.

**Certificates and FIPS compliance**

To be fully compliant with the 2011 recommendations for security strength, a minimum of 2,048/SHA256 certificates must be used. As the previous table indicates, only a new installation results in ePolicy Orchestrator server meeting the recommendations of the 2011 suggested certificate size.

When you replace the user interface server certificate on a server running in FIPS mode, ePolicy Orchestrator does not verify that the new certificate is FIPS-compliant. It is your responsibility to provide a compliant certificate.

Versions of Microsoft Windows released prior to Windows Vista do not support SSL certificates using SHA256 digests or 3,072-bit keys. Internet Explorer uses the Windows cryptography library, and as a result is unable to connect to an ePolicy Orchestrator server running in FIPS mode when the browser is running on older operating systems. Firefox uses its own cryptography library and is able to connect to a FIPS-mode ePolicy Orchestrator server from those older operating systems.

**FIPS mode behavior at startup**

When running in FIPS or Transition mode, ePolicy Orchestrator performs extra security checks at startup.

To maintain a secure boundary around the cryptographic modules, all ePolicy Orchestrator executables and all executables for extensions that are part of the ePolicy Orchestrator security module, or interact with it in any way, must be digitally signed. This signature is contained in a separate file that has the same name as the executable, plus a .sig extension. The same is true for the McAfee Agent, all of the programs that it runs, or uses, and any of its cryptographic functions, they all must also be digitally signed.

Consider the executable and the signature file to be a matched set. If you update one of these executables through a patch or any other means, you must update both files.
**ePolicy Orchestrator server startup behavior**

When the ePolicy Orchestrator server starts in FIPS mode, it performs the following initializations and self-checks:

- Verify that the CryptoJ module is running in FIPS mode and self-checks pass.
- Verify that CryptoJ and SSL-J are configured properly.
- Delete executables found in temporary directories.
- Verify that the RSA SSL-C module is running in FIPS mode and self-checks pass.
- Verify the server and extension executables.

If any of these fail verification, the following happens:

- The server (or server module if running within Apache) shuts down.
- The event parser service does not start.
- The Apache service does not process agent requests.
- Other unaffected modules in the Apache server continue to function.
- Log entries are made in `orion.log`, `eventparser.log`, `server.log`, and `epoapsvr.log`, depending on the verification step failure.

**Agent startup behavior**

When the agent starts on a client system in FIPS mode, it performs the following initializations and self-checks:

- Verify that all self-checks pass.
- Verify that the cryptography modules are configured properly.
- Verify that critical functions pass a security check.

Log entries are made in `Agent_<machinename>.log` or `McScript.log`.

---

**Secure Socket communication in FIPS mode**

FIPS mode requires particular secure protocols when communicating with the ePolicy Orchestrator server.

SSL communication can use different versions of different cryptographic protocols, if both the client and server support them. The primary protocols are Secure Sockets Layer (SSL) and Transport Layer Security (TLS). ePolicy Orchestrator 4.6 supports specific versions of these protocols, depending on its operating mode.

**Table 3-3 Supported communication protocols and ciphers**

<table>
<thead>
<tr>
<th>Category</th>
<th>FIPS and Transition mode</th>
<th>Mixed mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed protocols</td>
<td>TLS 1.0 only</td>
<td>TLS 1.0, SSL 3.0 and older</td>
</tr>
<tr>
<td>Allowed ciphers</td>
<td>FIPS-compliant ciphers specified in <code>server.xml</code></td>
<td>Any cipher specified in <code>server.xml</code></td>
</tr>
</tbody>
</table>

Note: TLS versions 1.1 and 1.2 are not supported.
McAfee products that support FIPS mode

These McAfee products are known to be compatible with FIPS mode.

<table>
<thead>
<tr>
<th>Product</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePolicy Orchestrator</td>
<td>4.6.0 through 4.6.4</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>4.6.0</td>
</tr>
<tr>
<td>McAfee Host Intrusion Prevention</td>
<td>8.0 Patch 1</td>
</tr>
<tr>
<td>McAfee Policy Auditor</td>
<td>5.3</td>
</tr>
<tr>
<td>McAfee VirusScan Enterprise</td>
<td>8.8</td>
</tr>
</tbody>
</table>

Products released by McAfee before 2011 are most likely not FIPS-compatible unless listed here. For other products, check that product's documentation for further information.
Index

A
about this guide 5
Agent Handlers
  certificate strength and encryption levels 19
  FIPS compliance 17

B
BMC Remedy Action Request System
  FIPS issues 17

C
Certificate hierarchy
  strength and encryption levels 19
Configuration files
  FIPS entries 19
conventions and icons used in this guide 5
Cryptographic boundary
  definition 11
  how products violate it 11

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

E
ePolicy Orchestrator
  FIPS compliance levels 10
  FIPS mode startup failures 20
  FIPS operating modes 10

F
FIPS
  comparing operating modes 10
  compliance levels 7
  introduction 7
  online availability 7
FIPS compliance
  Agent Handlers 17
  certified products 22

FIPS compliance (continued)
  cryptographic boundary 11
  ePolicy Orchestrator compliance levels 10
  maintaining 17
  managing non-compliant packages 17
  McAfee recommendations 17
  software requirements 12

FIPS mode
  certificate strengths 19
  certified products 22
  configuration file entries 19
  definition 10
  determining current 19
  installation 13
  log files used 20
  software requirements 12
  startup behavior 20
  supported communications protocols 21
  troubleshooting 20
  upgrading from a previous version of ePolicy Orchestrator 14
  user interface indicators 19

H
Hewlett-Packard OpenView ServiceDesk
  FIPS issues 17

I
Installation
  command-line option 13, 15
  FIPS mode 13
  McAfee Agent 16
  required agent upgrades 16
  Transition mode 15, 16
  upgrade from ePolicy Orchestrator 4.5 15
  upgrading from ePolicy Orchestrator 4.0 16

M
McAfee Agent
  FIPS mode log files used 20
  FIPS mode startup behavior 20
  FIPS-certified versions 22
  Installation 16
McAfee Agent (continued)
required upgrades 16
SSL connections after upgrade 15
McAfee Host Intrusion Prevention
FIPS-certified versions 22
McAfee Policy Auditor
FIPS-certified versions 22
McAfee ServicePortal, accessing 6
McAfee VirusScan Enterprise
FIPS-certified versions 22
Mixed mode
  certificate strengths 19
definition 10

R
Rogue System Detection
  certificate strength and encryption levels 19

S
ServicePortal, finding product documentation 6
SSL certificates
  ePolicy Orchestrator support 15
 SSL certificates (continued)
  strength and encryption levels 19
  upgrading from ePolicy Orchestrator 4.0 15
SSL communication
  supported ciphers 21
  supported protocols 21
Supported browsers 12
Supported operating systems 12

T
Technical Support, finding product information 6
Transition mode
  certificate strengths 19
definition 10
  installation 15, 16
  software requirements 12
Transport Layer Security (TLS)
  supported versions 21
Troubleshooting
  startup failures 20