# Symantec™ Endpoint Protection version 12.1.1000 FIPS 140-2 Deployment Guide

# Symantec Endpoint Protection version 12.1.1000 FIPS 140-2 Deployment Guide



Documentation version 12.1.1000

## Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

# Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

## Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

## Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

## Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

## Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

| | |
|---|---|
| Asia-Pacific and Japan | customercare_apac@symantec.com |
| Europe, Middle-East, and Africa | semea@symantec.com |
| North America and Latin America | supportsolutions@symantec.com |

# Contents

Chapter 1

# Introduction

This chapter includes the following topics:



## About Symantec Endpoint Protection and FIPS 140-2 level 1 compliance

Deploying Symantec Endpoint Protection in a FIPS-compliant configuration includes protecting the following types of communications:

- Client-to-server
- Server-to-server
- Remote administration

Symantec Endpoint Protection Release 12.1 RU 1 provides the Symantec Cryptographic Module cryptography library modules to protect server-to-server communication and console-to-server communication. It provides the Microsoft FIPS modules to protect client-to-server communication. You can deploy Symantec Endpoint Protection and protect its key command and control communications with NIST FIPS-validated security modules.

By default, the use of SSL is enabled in new installations, primarily for client-to-server reporting communication.

Once you complete the processes that are outlined here, the Symantec Cryptographic Module protects server-to-server communication, and the Microsoft FIPS modules protect client-to-server communication. Communication with the database, however, is in plaintext. Database communications should be protected by creating a closed network environment.

The Microsoft FIPS module that was used to protect client-to-server communication in Symantec Endpoint Protection version 11, RU 6a MP2 and later releases of version 11 has been maintained for compatibility with migrated installations.

These deployment instructions make the following assumptions:

- You have a typical enterprise network environment where Microsoft domain controllers are used to provide certificates from a domain controller certificate authority.
- The certificate authority is configured as an enterprise certificate authority that can fulfill certificate requests online to servers that are in the domain.

# Setting up your network and Symantec Endpoint Protection for FIPS 140-2 compliance

Symantec assumes that you have a typical enterprise network environment.

Figure 1-1 illustrates a large-scale deployment with multiple datacenters and Symantec Endpoint Protection Manager sites.

A private VLAN network protects database communication within the datacenter. FIPS-validated modules protect communication to Symantec Endpoint Protection clients and between sites on the intranet.

**Figure 1-1** Example network setup

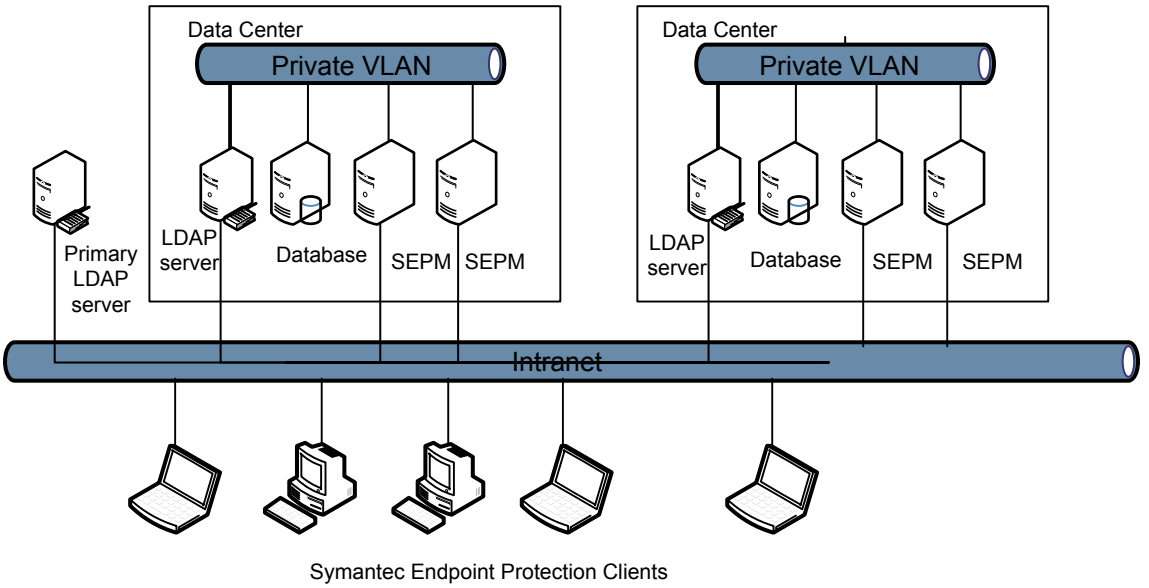


Table 1-1 outlines the tasks to set up your network and deploy Symantec Endpoint Protection for FIPS 140-2 compliance.

**Note:** You must upgrade to Symantec Endpoint Protection 12.1 RU 1 before you deploy the new libraries and executables for FIPS 140-2 compliance.

**Table 1-1** Setting up your network and deploying the software

| Step | Task | Description |
|---|---|---|
| Step 1 | Upgrade the Symantec Endpoint Protection Manager to version 12.1, RU 1 | You must upgrade to Symantec Endpoint Protection 12.1 RU 1 to get the latest Java and Apache libraries and executables and the deployment script. You can install for the first time, or you can upgrade. If you install for the first time, be sure to run the Management Server Configuration Wizard before you deploy in FIPS mode to avoid certificate problems.<br><br>For information about how to upgrade the Symantec Endpoint Protection Manager, see the upgrade instructions in the installation guide:<br><br>Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide |

**Table 1-1** Setting up your network and deploying the software *(continued)*

| Step | Task | Description |
|---|---|---|
| Step 2 | Protect client-to-server communication | To protect client to server communication, you need to enable FIPS mode in the local security policy. You also need to use Symantec Endpoint Protection Manager to create an SSL port for clients and to configure the clients to use HTTPS. You then deploy the new communications settings to the client and verify that they operate properly.<br>See "Protecting client-to-server communication" on page 14. |
| Step 3 | Protect server-to-server communication | To protect server to server communication, you need to install the FIPS-compliant Java and Apache libraries and executables (OpenSSL), and then verify that they are used.<br>See "Protecting server-to-server communication" on page 23. |
| Step 4 (optional) | Protect remote administration communication | If you want to use the remote console to manage Symantec Endpoint Protection, you must take some additional steps.<br>See "Protecting remote administration communication" on page 28. |

Chapter 2

# Deploying Symantec Endpoint Protection for FIPS 140-2 level 1 compliance

This chapter includes the following topics:



## Installing, upgrading, or migrating to Symantec Endpoint Protection version 12.1 RU1

Symantec Endpoint Protection 12.1 did not include support for FIPS 140-2 level 1. You can upgrade from version 12.1 to version 12.1 RU1 to get the Java and Apache libraries and the deployment script that provide support for FIPS 140-2 level 1. You can install version 12.1 RU1 for the first time, or you can upgrade from version 12.1.

Symantec Endpoint Protection version 1.0 RU 6 MP2 and later versions contained support for FIPS 140-2 level 1 communications, but you can migrate to 12.1 RU1

from any version of Symantec Endpoint Protection 11.X, regardless of whether it contains FIPS 140-2 level 1 support.

---

**Note:** If you upgrade a server that is in FIPS mode from Symantec Endpoint Protection 11.0.6a MP 2 or later releases of version 11, that server remains in FIPS mode.

---

The Symantec Endpoint Protection 11.X releases that support FIPS 140-2 level 1 use IIS for client-to-server communications. Version 12.1 RU1 uses Apache for client-to-server communications.

Apache serves Symantec Endpoint Protection reports on port 8445. When migrating, follow the user guide instructions on checking for ports in use. If port 8445 is currently in use, then you should change the reporting Web site to use a different port during the migration process.

---

**Note:** If you install for the first time, be sure that you run the Management Server Configuration Wizard before you deploy and enable the FIPS-compliant Java and Apache libraries and executables to avoid certificate problems.

If you need to run the Management Server Configuration Wizard after you deploy and enable the FIPS-compliant Java and Apache libraries and executables, you should disable the libraries beforehand.

See "Deploying and using FIPS-compliant mode" on page 25.

---

For information about upgrading Symantec Endpoint Protection, see the upgrading chapter of the Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide.

# Protecting client-to-server communication

After you have upgraded or installed Symantec Endpoint Protection 12.1 RU1 or later version, you need to configure protection for client-to-server communication.

**Table 2-1** Tasks that you need to perform to protect client-to-server communication

| Step | Task | Description |
|---|---|---|
| Step 1a | Enable FIPS mode in the local Windows security policy. | For information about how to enable FIPS mode in the local security policy, look for the section called "Instructions on Setting the FIPS Local Policy Flag" on the following Web page:<br>FIPS 140 Evaluation<br>The following Web page also contains some instructions on how to set the FIPS Local Policy Flag on Windows Server 2003 or 2008 and Windows XP and Vista.<br>Instructions for using SQL Server 2008 in FIPS 140-2-compliant mode |
| Step 1b | Enable Internet Explorer TLS 1.0 on Windows 2003. | If the operating system in use is Windows 2003, you must open Internet Explorer and use the **Advanced** tab on the Internet Explorer **Tools > Internet Options** menu to enable TLS 1.0. |
| Step 2 | Verify that Windows operates in FIPS mode. | See "Verifying that Windows operates in FIPS mode" on page 18.<br>For additional information about how to verify that Windows operates in FIPS mode, see the following Web page:<br>PRB: Cannot visit SSL sites after you enable FIPS compliant cryptography<br>General information is located on the following Web page:<br>The effects of enabling the "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting in Windows XP and in later versions of Windows |

**Table 2-1** Tasks that you need to perform to protect client-to-server communication *(continued)*

| Step | Task | Description |
|---|---|---|
| Step 3 | Enable SSL communications between the clients and Symantec Endpoint Protection Manager. | Enable SSL communications between the clients and Symantec Endpoint Protection Manager.<br>**Note:** If you want to upgrade from version 11 RU6a MP2 or a later release where you had FIPS mode enabled, then it is considered a best practice to reconfigure your clients to use the new connection infrastructure. Version 11 RU6a MP2 and later 11.X releases used custom IIS ports to communicate to the clients over a TLS connection. Custom ports are not migrated during the installation to use the new Apache-based client communication infrastructure.<br>■ Check the ports currently in use and change the default Apache SSL port, if desired.<br>See "Checking and changing the Apache SSL port" on page 18.<br>■ Enable and verify the SSL port on Symantec Endpoint Protection Manager.<br>See "Enabling and verifying the SSL port on Symantec Endpoint Protection Manager" on page 19.<br>**Note:** Symantec Endpoint Protection version 11, RU 6a MP2 and later 11.X releases used IIS rather than Apache. Information about assigning certificates to the IIS HTTPS port using an online domain certificate authority is still available in the following source:<br>Symantec Endpoint Protection version 11, RU 6a, MP 2 and later FIPS 140-2 Deployment Guide |
| Step 4 | Create an HTTPS management server list. | To secure client-to-server communications, you must configure Symantec Endpoint Protection Manager to use HTTPS over the Apache port instead of the default protocol, HTTP. If you are migrating from a version 11.X release that supports FIPS mode, you can edit your existing management server list and replace the existing IIS port with the Apache port. When you save the edited management server list, Symantec Endpoint Protection Manager sends that information at the next update to connected clients so that they can reconnect over the new port.<br>See "Enabling SSL on the clients by adding a management server list" on page 20. |

**Table 2-1** Tasks that you need to perform to protect client-to-server communication *(continued)*

| Step | Task | Description |
|---|---|---|
| Step 5 | Install certificates on the clients so that they can verify the certificates. | If your clients do not inherently trust your certificate authority, then you should install certificates on the clients so that they trust your certificate authority.<br>If you have not enabled the Symantec Endpoint Protection group's option to verify the server certificate in the **General Settings** dialog box on the **Security Settings** tab, then you should not need to perform this task.<br>If you do need to perform this step, see the following Web page:<br>Distribute your own Certificate Authority cert via group policy. |
| Step 6 | Assign the HTTPS management server list to the top-level group. | You must assign the management server list to the client groups so that Symantec Endpoint Protection Manager uses HTTPS when it sends policies to the clients.<br>See "Assigning a management server list to the top-level group" on page 22.<br>**Note:** If you have already deployed a client that uses HTTP, it automatically switches to HTTPS at the next update from the server. In this case, you do not need to perform steps 7 and 8. |
| Step 7 (optional) | Use the Migration and Deployment Wizard to create a client package. | For information about creating a client package, see the "Installing the Symantec Endpoint Protection client" chapter of the following guide:<br>Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide. |
| Step 8 (optional) | Deploy the client package to the client computers. | For information about deploying client packages, see the "Installing the Symantec Endpoint Protection client" chapter of the following guide:<br>Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide. |
| Step 9 | Verify that the clients use SSL to connect. | Once you deploy clients or edit your existing management server list to route client communications through the Apache port, verify that they use SSL to connect.<br>See "Verifying that clients use SSL to connect to Symantec Endpoint Protection Manager" on page 22. |

## About enabling Windows FIPS mode on clients and servers

A FIPS-mode security policy must be enabled on the Windows client computers and the Windows servers to properly protect communications. The FIPS policy setting restricts the Windows components to use of approved ciphers. Microsoft

recertifies FIPS binaries for each release. These components rely on the Rsaenh.dll validated module.

For an overview and a certification table by operating system release, see the following Web page:

FIPS 140 Evaluation

## Verifying that Windows operates in FIPS mode

**To verify that Windows operates in FIPS mode**

1. Open Internet Explorer.
2. Click **Tools**, and then click **Internet Options**.
3. Uncheck **Use TLS 1.0** and leave **Use SSL 3.0** checked.
4. Click **OK**.
5. Browse to the following URL:

   **https://SepmServer:8443/**

   If the RSA libraries are in use, you should see an error and the page should not display.

## Checking and changing the Apache SSL port

The default SSL port for Apache is port 443. If you want clients to use the default port to communicate with Symantec Endpoint Protection Manager, you should first check to see if that port is available. You may want to use a different port for new installations to minimize conflict with any applications that already use the default SSL port.

**To see if the default port is available**

- Open a command window and type the following command:

  **netstat -an | find ":443"**

  If the `netstat` command returns 443 in the list of ports in use, you must change the port entry in the sslForClients.conf file to an unused port.

If you know that you want to change the port to be used for SSL communication, check to see what ports are already in use.

**To see the list of ports that are currently in use**

- Open a command window and type the following command:

  **netstat -an**

  Be sure to pick a port for SSL that is not already in use.

If you want to change the port number, use the following procedure.

**To change the Apache SSL port for client communication**

1. Open the *drive*:*install_directory*\Symantec\Symantec Endpoint Protection Manager\apache\conf\sslForClients.conf file with a text editor.
2. Locate the following line:

   ```
   Listen 443
   ```

3. Change the number to an unused port. For example, you can change it to 4431, if that port is not already in use by another application.

   Listen *4431*

4. Locate the following line:

   ```
   <VirtualHost _default_:443>
   ```

5. Change the number to the same port you used for the **Listen** entry. For example, change it to 4431.

   ```
   <VirtualHost _default_:4431>
   ```

6. Save the file and close the text editor.

---

**Note:** Now you can log into Symantec Endpoint Protection Manager and create or modify a management server list to use the SSL port that you configured in the sslForClients.conf file. Symantec recommends that you avoid use of the **Verify certificate when using HTTPS protocol** option unless you are very familiar with certificates and their usage.

---

## Enabling and verifying the SSL port on Symantec Endpoint Protection Manager

**To enable the SSL port on Symantec Endpoint Protection Manager**

1. Open the *drive*:*install_directory*\Symantec\Symantec Endpoint Protection Manager\apache\conf\httpd.conf file with a text editor.
2. Locate the following line in the file:

   ```
   #Include conf/ssl/sslForClients.conf
   ```

3 Delete the pound sign (#) to uncomment the line:

```
Include conf/ssl/sslForClients.conf
```

4 Save the file and close the text editor.

**To verify that the port has been changed**

1 Restart the Symantec Endpoint Protection Manager Webserver service by opening a command window and typing the following commands:

**net stop semwebsrv**

**net start semwebsrv**

Restarting the Webserver service also restarts the Symantec Endpoint Protection Manager service, as it depends on the Symantec Endpoint Protection Manager Webserver.

2 Open a Web browser and ensure that the following URL returns OK:

```
https://ServerHostname:new_port/secars/secars.dll?hello,secars
```

If it does, then Apache now listens on the new port.

---

**Note:** To ensure that clients communicate with Symantec Endpoint Protection Manager over the new port, you need to modify a management server list to use the new port number. Then you need to apply the list to the clients.

See "Enabling SSL on the clients by adding a management server list" on page 20.

---

## Enabling SSL on the clients by adding a management server list

The management server list specifies the order in which clients in a particular group connect. Clients first try to connect to the management servers that have been added with the highest priority.

To operate in FIPS-compliant mode, you should use HTTPS communication in place of HTTP communication. Symantec recommends that you use a different port for new installations to minimize conflict with any applications that use port 443, the default HTTPS port. If you change the HTTPS port after you deploy clients, you must update the client configuration files so that clients connect over the new port.

After you add a new management server list, you must assign it to a specific group or location or both.

**Note:** If you are migrating from an earlier version 11 release that supports FIPS mode, you can edit an existing management server list and replace the IIS port that you used with the new Apache SSL port.

See "Assigning a management server list to the top-level group" on page 22.

**To enable SSL on the clients by adding a management server list that uses HTTPS**

1. In the console, click **Policies**.
2. In the **Policies** page, under **View Policies**, click **Policy Components > Management Server Lists**.
3. Under **Tasks**, click **Add a Management Server List**.
4. In the **Management Server Lists** dialog box, in the Name text field, type a name for the management server list and an optional description.
5. Select **Use HTTPS protocol**.
6. If you require verification of a certificate with a trusted third-party certificate authority, check **Verify certificate when using HTTPS protocol**.

   **Note:** If you do not require verification, deployment takes fewer steps.

7. To add a server, click **Add > New Server**.
8. In the **Add Management Server** dialog box, in the **Server address** text field, type the IP address or host name of the management server.
9. If you changed the port number from 443 in the sslForClients.conf file, check **Customize HTTPS port number**, and then type in the new port number. For example, you can use port 4431, if it is not already in use by another application. Be sure to use the same port that you configured in the sslForClients.conf file.

   **Note:** If you customize the HTTPS port number after you deploy the client software, the clients lose communication with the management server. They reestablish communication after the next client update from the server, which contains the new connection information.

10. Click **OK**.
11. If you need to add a management server that has a different priority than the management server that you added, click **Add > New Priority**.

12 Repeat steps 7 through 10 to add more management servers.

13 In the **Management Server Lists** dialog box, click **OK**.

## Assigning a management server list to the top-level group

After you add a management server list, you can assign it to the top-level group.

**To assign a management server list to the top-level group**

1 In the console, click **Policies**.

2 In the **Policies** page, under **View Policies**, click **Policy Components > Management Server Lists**.

3 In the **Management Server Lists** pane, select the management server list that you created to use HTTPS.

4 Under **Tasks**, click **Assign the List**.

5 In the **Apply Management Server List** dialog box, click the top-level group.

6 Click **Assign**.

7 When you are prompted, click **Yes**.

## Verifying that clients use SSL to connect to Symantec Endpoint Protection Manager

You can verify that the clients use SSL to connect to Symantec Endpoint Protection Manager.

**To verify that a client connects over SSL using a Web browser**

- On the client, open a Web browser and type the following URL:

  `https://`*`ServerHostname`*`:`*`port_number`*`/secars/secars.dll?hello,secars`

  Be sure that you use the host name and not the IP address.

  If it returns an OK message, and there are no certificate warnings from the Web browser, then the certificate is trusted and current, and communication takes place over SSL.

  **Note:** If the client cannot resolve your server's host name, you can add the host name and IP address to the client's Windows hosts file.

**To verify that a client connects over SSL using the client user interface**

1. Open the client user interface and click **Help > Troubleshooting**.
2. In the **Troubleshooting** window, click **Connection Status** and check the server name and port over which the client last successfully connected.

   If the client did not connect through the SSL port number, you can click **Connect Now** to have the client request to connect to Symantec Endpoint Protection Manager.

# Protecting server-to-server communication

Server-to-server communication occurs on port 8443. The Symantec Cryptographic Module (Software Version: 1.0) provides FIPS-certified communication on both the server and the client sides of the Symantec Endpoint Protection Manager to Symantec Endpoint Protection Manager connections.

**Table 2-2** Tasks that you need to perform to protect server-to-server communication

| Step | Task | Description |
|---|---|---|
| Step 1 | Install or upgrade to Symantec Endpoint Protection 12.1 RU 1 or later version. | If you have not already installed or upgraded to Symantec Endpoint Protection 12.1 RU 1 or later version, you must do so before you deploy the FIPS-compliant Java libraries.<br>**Note:** If you install for the first time, be sure to run the Management Server Configuration Wizard to complete the configuration of the Symantec Endpoint Protection Manager. Using the Management Server Configuration Wizard for configuration before you deploy and enable the FIPS-compliant Java libraries can help to avoid certificate problems.<br>For information about upgrading Symantec Endpoint Protection, see the upgrading and migrating chapter of the following guide:<br>Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide. |
| Step 2 | Back up your server certificate. | A best practice is to back up your server certificate. Then, even if you inadvertently overwrite your server certificate with an invalid certificate, you can restore the valid one.<br>For information about backing up a server certificate, see the section named "Backing up a server certificate" in the following guide:<br>Symantec Endpoint Protection and Symantec Network Access Control Implementation Guide. |

**Table 2-2** Tasks that you need to perform to protect server-to-server communication *(continued)*

| Step | Task | Description |
|---|---|---|
| Step 3 | Deploy the FIPS-compliant Java and Apache libraries and executables. | Symantec provides a script file to install the libraries and executables.<br>**Note:** You must upgrade to Symantec Endpoint Protection12.1 RU 1 or later version and configure Symantec Endpoint Protection Manager before you install the libraries.<br>See "Deploying and using FIPS-compliant mode" on page 25. |
| Step 4 | Verify that the RSA libraries are in use for server-to-server communications. | To ensure that the RSA libraries are in use for server to server communications, you can verify that SSL V3 is not used.<br>See "Verifying that communications are FIPS-compliant" on page 26. |

## About the FIPS-compliant Java libraries

Symantec provides a script file to install the libraries. The script file takes the following actions:

- Stops Symantec Endpoint Protection Manager service and the Symantec Endpoint Protection Manager Webserver service.
- Installs the Sun JCE Unlimited Strength Jurisdiction Policy jars to the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\jre\lib\security folder.
- Installs the FIPS-compliant Java and Apache libraries and executables.
- Updates the java.security file that is located in the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\jre\lib\security folder to install the JCE provider libraries.
- Enables the FIPSMode option in the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\apache\conf\ssl\ssl.conf file.
- Specifies the use of FIPS mode in the *drive*:\Program Files\Symantec\Symantec Endpoint Protection Manager\Tomcat\etc\conf.properties file.
- Adds the following line to configure the pseudo random number generator algorithm to a secure, performant version to the java.security file:
  com.rsa.crypto.default.random=HMACDRBG256
- Restarts the Symantec Endpoint Protection Manager service and the Symantec Endpoint Protection Manager Webserver service.

This release uses RSA Crypto-J 5.0, Apache 2.2.19, OpenSSL 0.9.8r (also referred to as 0.9.8.18), and RSA SSL-J 5.1.1.1. When operating in non-FIPS mode, it uses RSA Crypto-J 4.1.

For FIPS certificate and security policy information, see the following Web page:

Symantec Cryptographic Module (Software Version: 1.0)

## About the validated modules

The Symantec Endpoint Protection deployment uses the validated modules that are listed in Table 2-3.

**Table 2-3** The modules and the components that they protect

| NIST CMVP module certificate number and description | Protected components |
|---|---|
| 1008, 1009, 1010 – Microsoft bcrypt.dll, DSSENH, RSAENH | ■ Symantec Endpoint Protection clients, by WinINet and SChannel<br>■ Remote desktop |
| Symantec Cryptographic Module | ■ Symantec Endpoint Protection Manager Tomcat server Java JCE module<br>■ Symantec Endpoint Protection Manager Java console JCE module |

## Deploying and using FIPS-compliant mode

You can use a Symantec-supplied script to deploy, enable, disable, and reapply FIPS-compliant mode. You can double-click the script to check the current FIPS state, on or off. You can also use the FIPSMode.vbs script's `-reapply` flag to repair FIPS mode after an upgrade or after other changes.

A best practice is to log out of the Java console before you use the FIPSMode enable command or disable command. If you do not log off, you may see an error message that states that you cannot connect to the server. This message occurs because the FIPSMode commands temporarily stop both the server service and the Web server service. You can safely ignore this message and click **OK** in the message box.

**Note:** If you need to run the Management Server Configuration Wizard after you deploy and enable the FIPS-compliant Java and Apache libraries and executables, you should first disable the libraries.

**To deploy and enable the FIPS-compliant Java libraries**

1. Change folder to the *drive*:*install_directory*\Program Files\Symantec\Symantec Endpoint Protection Manager\bin folder.
2. Double-click the FIPSMode-Enable.bat file.

**Note:** You can repeat this operation any number of times with no adverse consequences.

**To disable the FIPS-compliant Java libraries**

1. Change folder to the *drive*:*install_directory*\Program Files\Symantec\Symantec Endpoint Protection Manager\bin folder.
2. Double-click the FIPSMode-Disable.bat file.

**Note:** You can repeat this operation any number of times with no adverse consequences.

You can use this option to repair or reapply the current FIPS state, either On or Off. This command does not change the current FIPS state, but it does silently redeploy the current FIPS state. It stops and restarts the Symantec Endpoint Protection Manager services as part of that redeployment.

**To reapply the FIPS-compliant Java and Apache libraries and executables**

- Open a command window and type the following command:

  **.\bin\FIPSMode.vbs -reapply**

## Verifying that communications are FIPS-compliant

To verify that the RSA libraries are in use for server to server communications, use the following procedure.

**To verify that communications are FIPS-compliant**

1. Open Internet Explorer.
2. Click **Tools**, and then click **Internet Options**.
3. Uncheck **Use TLS 1.0** and leave **Use SSL 3.0** checked.

4 Click **OK**.

5 Browse to the following URL:

**https://SepmServer:8443/**

If the RSA libraries are in use for server to server communications, you should see an error and the page should not appear.

---

**Note:** You can also use this procedure with the reporting Web site (port 8445) to verify FIPS-compliant mode operation.

---

Alternatively, if you do not want to turn off TLS 1.0, you can use the following OpenSSL command-line procedure to verify that communications are FIPS-compliant.

### To verify that communications are FIPS-compliant by using OpenSSL commands

1 Open a command window.

2 Type one of the following commands:

| | |
|---|---|
| To verify Tomcat SSL communications, typically on port 8443 | **openssl s_client -connect *server_name_or_ip_address*:*Tomcat_port_number* -ssl3** |
| To verify Tomcat TLS communications, typically on port 8443 | **openssl s_client -connect *server_name_or_ip*_address:*Tomcat_port_number* -tls1** |
| To verify Apache Reporting SSL communications, typically on port 8445 | **openssl s_client -connect *server_name_or_ip_address*:*Apache_port_number* -ssl3** |
| To verify Apache Reporting TLS communications, typically on port 8445 | **openssl s_client -connect *server_name_or_ip_address*:*Apache_port_number* -tls1** |

**Note:** You can also verify that communications are FIPS-compliant over client connections by substituting the number of the Apache HTTPS client port in the openssl command.

You can also specify a remote server name or IP address to verify that communications are FIPS-compliant on a different Symantec Endpoint Protection Manager. You might use that command if you want to verify that communications are FIPS-compliant on an existing 11 RU6 MP2 or later Symantec Endpoint Protection Manager from a newly installed 12.1 RU1 Symantec Endpoint Protection Manager.

# Protecting remote administration communication

You must perform some additional tasks if you want to maintain FIPS compliance and you plan to administer Symantec Endpoint Protection remotely.

**Table 2-4** Tasks that you need to perform to protect remote administration communication

| Step | Task | Description |
|---|---|---|
| Step 1 (optional) | Assign certificates to the HTTPS port by using an online domain certificate authority. | If you want to use the Symantec-generated default certificate, or if you have already performed this task, you can skip this step.<br>If you need to change the ports that Symantec Endpoint Protection Manager uses, see the following Web page:<br>Symantec Endpoint Protection 12.1: How to Change the ports used for communication between the Manager and clients |
| Step 2 | Ensure that you can navigate to and view the reporting Web site and the management Web site directly in Internet Explorer without an error. | See "Establishing certificate trust for the reporting Web site and the management Web site" on page 29. |
| Step 3 | Verify that the console operates in compliance. | You can disable the use of TLS to verify that the console uses HTTPS to operate in FIPS compliance.<br>See "Verifying that the Web sites operate in compliance" on page 30. |

**Table 2-4** Tasks that you need to perform to protect remote administration communication *(continued)*

| Step | Task | Description |
|---|---|---|
| Step 4 | Add your Symantec Endpoint Protection Manager server host name to the Internet Explorer **Local Intranet** zone.<br><br>If the remote console problem persists, then you can uninstall the Enhanced Security Configuration for Internet Explorer on the computer that runs the Web console. | Because the Web console uses AJAX Active Client scripting, it may help to add your Symantec Endpoint Protection Manager server host name to the Internet Explorer **Local Intranet** zone.<br><br>See "Adding your Symantec Endpoint Protection Manager server host name to the Local intranet zone" on page 31.<br><br>If you continue to have difficulty accessing the remote console, consider disabling Internet Explorer Enhanced Security on the computer that runs the Web console.<br><br>See "Disabling Enhanced Security Configuration on Windows 2003 servers" on page 31.<br><br>See "Disabling Enhanced Security Configuration on Windows 2008 servers" on page 32.<br><br>For additional information, see the following Web pages:<br><br>■ For Windows Server 2003:<br>Modifying Enhanced Security Configuration Settings<br>■ For Windows Server 2008:<br>Internet Explorer Enhanced Security Configuration |

## Establishing certificate trust for the reporting Web site and the management Web site

You need to establish certificate trust to use Internet Explorer to reach the reporting Web site and the management Web site.

**To establish certificate trust for the reporting Web site**

1. Navigate to the appropriate URL, for example:

   https://*hostname*:8445/Reporting/login/login.php
2. Click through the error and load the page.
3. Click the security report lock icon (Internet Explorer 7 or 8) to view the certificate.
4. Import the certificate into the trusted root certificate authorities store.

5 Reload the page and import the certificate again into the default certificate store.

**Note:** When you establish certificate trust, some browsers, such as Internet Explorer 8, may require that you restart the browser rather than refresh the page.

6 Reload the page again and verify that you no longer get a certificate error.

**To establish certificate trust for the management Web site**

1 Navigate to the appropriate URL, for example:

https://*hostname*:8443

2 Click through the error to load the page.

3 Click the security report lock icon (Internet Explorer 7 or 8) to view the certificate.

4 Import the certificate into the trusted root certificate authorities store.

5 Reload the page and import the certificate again into the default certificate store.

**Note:** When you establish certificate trust, some browsers, such as Internet Explorer 8, may require that you restart the browser rather than refresh the page.

6 Reload the page again and verify that you no longer get a certificate error.

## Verifying that the Web sites operate in compliance

You can verify that the management Web site and the reporting Web site use HTTPS to operate in FIPS compliance.

**Note:** If you customized the ports that are used, use those port numbers instead of the defaults.

**To verify that the Web sites operate in compliance**

1 Open Internet Explorer, click **Tools**, and then click **Internet Options**.

2 On the **Advanced** tab, scroll down to the Security section and uncheck **Use TLS 1.0**, if it is not already unchecked.

3 Close and then restart Internet Explorer.

4 To verify that the management Web site uses HTTPS for communication, try to browse to the following address:

https://*hostname*:8443/

To verify that the reporting Web site uses HTTPS for communication, try to browse to the following address:

https://*hostname*:8445/

If the RSA libraries are in use for remote administration communications, you should see an error and the page should not display.

## Adding your Symantec Endpoint Protection Manager server host name to the Local intranet zone

**To add your Symantec Endpoint Protection Manager server host name to the Local intranet zone**

1 Open Internet Explorer.

2 Go to Tools > Internet Options, and then click the **Security** tab.

3 Click **Local intranet**, and then click **Sites**.

4 In the **Local intranet** dialog box, click **Advanced**.

5 Type your Symantec Endpoint Protection Manager server host name in the **Add this website to the zone** text box. For example, you might type in SEPMServerHostname.com.

6 Click **Add**.

7 Type your Symantec Endpoint Protection Manager server IP address in the **Add this website to the zone** text box and then click **Add**.

8 Click **Close**.

9 Click **OK** until you return to Internet Explorer.

## Disabling Enhanced Security Configuration on Windows 2003 servers

**To disable Enhanced Security Configuration on Windows 2003**

1 In the **Control Panel**, double-click **Add or Remove Programs**.

2 Click **Add/Remove Windows Components**.

3. Click **Internet Explorer Enhanced Security Configuration**, and then click **Details**.
4. Select the group for which you want to disable Enhanced Security Configuration, and then click **OK**.

## Disabling Enhanced Security Configuration on Windows 2008 servers

**To disable Enhanced Security Configuration on Windows 2008 servers**

1. Log on to the computer with a user account that is a member of the local Administrators group.
2. Click **Start**, and then click **Administrative Tools**.
3. Click **Server Manager**.
4. If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue**.
5. Under **Security Information**, click **Configure IE ESC**.

   **Note:** Server Manager opens with the same window that was in use when it was last closed.

6. If you do not see the **Security Information** section, then click **Server Manager** in the console tree.
7. Under **Administrators**, click **Off**.
8. Under **Users**, click **Off**.
9. Click **OK**.
10. Restart Internet Explorer so that your Enhanced Security Configuration changes take effect.

Chapter 3

# Best practices and limitations

This chapter includes the following topics:



## Best practices for database communications

Database communications are plaintext. You should protect database communications by using a controlled environment that segregates database network packets onto a private network.

See Figure 1-1 on page 11.

You can use the following techniques to achieve this goal:

- Multiple NICs
- Link security
- A private network
- A private server VLAN
- A trusted datacenter with firewall protection

# Best practices when you use an LDAP server with Symantec Endpoint Protection

Symantec recommends the following practices when you use an LDAP server with Symantec Endpoint Protection:

- Enable LDAP SSL connections in Symantec Endpoint Protection Manager. See "Enabling SSL connections for an LDAP server" on page 34.
- Depending on your deployment topology, you may need to provide additional protection for LDAP server information to maintain FIPS-protected mode. You may need to provide additional protection by making a locally accessible replica within the protected environment if a FIPS module does not protect the LDAP server communications.

## Enabling SSL connections for an LDAP server

**To enable SSL connections for an LDAP server**

1. In the console, click **Admin**, and then click **Servers**.
2. Under **Servers**, click the appropriate management server.
3. Under **Tasks**, click **Edit the Server Properties for *server name***.
4. Click **Directory Servers**, and then click **Add**.
5. In the **Add Directory Server** dialog box, click **LDAP**.
6. Click **Use Secure Connection**.
7. Click **OK**.
8. Click **OK**.

**Note:** This connection may or may not be FIPS-encrypted, depending on the capabilities of the LDAP server.

# About the limitations on Symantec Endpoint Protection features

FIPS compliancy imposes some limitations on the following Symantec Endpoint Protection features:

- For Remote Management, Symantec recommends that you use the Web console or a connection that uses RDP to access the console locally on the server.

- Because of the increased load that TLS places on performance, Symantec recommends that you have the Symantec Endpoint Protection Manager manage a limited number of clients.
- Although you can connect Symantec Endpoint Protection Mac clients to your FIPS-mode server network, the Mac clients have not yet been upgraded to use a FIPS-validated client TLS encryption module.

# About the features that are not supported when you run Symantec Endpoint Protection in a FIPS-compliant manner

The following Symantec Endpoint Protection features have not been analyzed or tested for use in a Symantec Endpoint Protection 12.X-based FIPS-compatible deployment at this time:

- Group Update Providers
- Quarantine servers
- The Symantec Network Access Control Enforcer appliance

As a best practice, do not use these Symantec Endpoint Protection features if you want to ensure that you maintain a FIPS-protected environment.

When recovering from a disaster, note that if your site was in FIPS mode, you must reenable FIPS mode manually. Be sure to double-click the FIPSMode-Enable.bat file to redeploy the libraries and executables and reenable FIPS mode.

Appendix A

# Troubleshooting SSL communication problems

This appendix includes the following topics:



## Issue: New client installations cannot connect to the server

Probable cause: The firewall disabled the HTTP ports on the server. This issue may occur if you use one of the Symantec Endpoint Protection Manager client deployment methods to deploy the client software packages. The clients may be assigned to the default server group, which uses HTTP.

Solution: Change the server connection setting in the sylink.xml file in the client package to use HTTPS and the HTTPS port and then redeploy the package. For example, if the server address setting is as follows:

**<Server Address="[hostname]" HttpPort="8014" HttpsVerifyCA="0" VerifySignatures="1" />**

Then change the server address to the following setting:

**<Server Address="[hostname]" HttpsPort="8445" HttpsVerifyCA="0" Protocol="HTTPS" VerifySignatures="1" />**

# Issue: The management console displays a certificate error when it tries to connect to the SSL reporting site

Probable cause: The Web browser and management console use embedded browser frames. To avoid certificate errors, the access URLs must be configured to use a host name that matches the server certificate. The embedded browser must trust the certificates and the certificate authorities that are used to sign them.

Solution: To resolve this issue, work your way through the steps that are outlined in Table A-1.

**Table A-1** Steps to resolve a certificate error

| Step | Task | Description |
|---|---|---|
| Step 1 | Ensure that you have modified the sesm.bat file to contain the server name. | Locate the procedure to "Change default server in SEPM logon console," in the following knowledge base article, and follow those instructions:<br>Configuring Secure Sockets Layer (SSL) to work with the Symantec Endpoint Protection reporting functions on Windows Server 2003 |
| Step 2 | Ensure that the server name and HTTPS settings are correct in the conf.properties file. | Scroll down to the section titled "Manually Editing of conf.properties file" in the following knowledge base article, and follow the instructions:<br>Configuring Secure Sockets Layer (SSL) to work with the Symantec Endpoint Protection reporting functions on Windows Server 2003 |

**Table A-1** Steps to resolve a certificate error *(continued)*

| Step | Task | Description |
|---|---|---|
| Step 3 | Ensure that you can navigate to the reporting Web site directly in Internet Explorer without an error. | If you get an error, take the following actions:<br>■ Navigate to the appropriate URL, for example, https://*hostname*:8445/Reporting/login/login.php.<br>■ Click through the error and load the page.<br>■ Click the security report lock icon (Internet Explorer 8) to view the certificate.<br>■ Import the certificate into the trusted root certificate authorities store.<br>■ Reload the page and import the certificate again into the default certificate store.<br>■ Reload the page again and verify that you no longer get a certificate error. |
| Step 4 | Ensure that you can navigate to the management Web site directly in Internet Explorer without an error. | If you get an error, take the following actions:<br>■ Navigate to the appropriate URL, for example, https://*hostname*:8443.<br>■ Click through the error to load the page.<br>■ Click the security report lock icon (Internet Explorer 8) to view the certificate.<br>■ Import the certificate into the trusted root certificate authorities store.<br>■ Reload the page and import the certificate again into the default certificate store.<br>■ Reload the page again and verify that you no longer get a certificate error. |

# Issue: After installing the Symantec Endpoint Protection Manager and FIPS Java libraries, console logon fails with the error "Failed to connect to the server"

Possible Cause: This issue can occur if you deploy the Java FIPS libraries before you run the Management Server Configuration Wizard. The Java FIPS library deployment script checks that the Symantec Endpoint Protection Manager service is installed before it deploys the FIPS Java libraries to prevent this issue.

Solution: Uninstall Symantec Endpoint Protection Manager and the libraries, and then reinstall in the correct order.

# Issue: Symantec Endpoint Protection Manager receives the error "reporting components could not be initialized"

Possible cause: The TLS protocol is not enabled.

Solution: Open Internet Explorer and click Tools > Internet Options > Advanced. Scroll down to the Security section and check the checkbox for the Use TLS 1.0 option.

# Issue: My Symantec Endpoint Protection client does not connect to the server

Possible cause: Some versions of Microsoft products default to a state where TLS 1.0 use is disabled, regardless of how you configure that value on the computer. You may see that the **Use TLS 1.0** option under the **Tools >Internet Options> Advanced > Security** menu is checked, but the service may still continue to use the program default.

Solution: Change the SecureProtocols registry value for the local system account. You may want to deploy this change to all clients by using a Windows group policy.

Exported into a .reg file, the value should look as follows:

**Windows Registry Editor Version 5.00**

**[HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings] "SecureProtocols"=dword:000000a8**

# Issue: I can't log on to the server after setting up a deny list under server properties

Possible cause: You ignored the error "**Your Console Access settings as provided will deny access to the current system. Do you want to continue?**." When you used SSL to connect to the server, your IP address was not the localhost address, but one of the server's addressable IP addresses.

Solution: To log back in, connect to the server using localhost or 127.0.0.1. Then manually add IP entries for the local server and the client computers that require server access.

# Issue: On a multi-homed network or a network that uses multiple IP addresses, the remote Web console cannot reach the reporting Web site

Possible cause: The Web console has selected an unroutable IP address from the list of network connections. The Web console uses the first IP address in the list in URLs.

Solution: Make the externally routable IP address appear first. For example, you can do one of the following tasks:

- Reorder the IP addresses that are assigned to the NIC so that the externally routable IP address appears at the top of the list.
- Change the binding order of the NICs.

---

**Note:** Depending on how your network is set up, reordering the network interfaces may affect other aspects of your environment. We recommend that you determine the effects of the reordering for your network before you make any changes.

---

For information about how to change the NIC binding order for Windows XP/2000, see the following Web page:

How to change the binding order of network adapters in Windows XP and in Windows 2000

For information about how to change the ordering of interfaces for Windows 2003/2008, see the following Web page:

Change the interface metric on a network adapter

**Issue: On a multi-homed network or a network that uses multiple IP addresses, the remote Web console cannot reach the reporting Web site**