Symantec Endpoint Encryption Upgrade Guide

Version 11.2.0

Preface

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Document version: 11.2.0

Document release date: April 2018

Contents

Chapter 1

Prerequisites for Upgrading Symantec Endpoint Encryption

This chapter includes the following topics:

Symantec Endpoint Encryption system requirements

Review the Symantec Endpoint Encryption system requirements before you perform an installation or upgrade.

Table 1-1 Symantec Endpoint Encryption system requirements

System requirements	Article URL
Symantec Endpoint Encryption Management Server system requirements	http://www.symantec.com/docs/INFO3168
Symantec Endpoint Encryption Client system requirements	http://www.symantec.com/docs/INFO3170
Symantec Endpoint Encryption Management Console system requirements	http://www.symantec.com/docs/INFO3169

Symantec Endpoint Encryption protocols and ports

The following table identifies each protocol and port that is used by Symantec Endpoint Encryption.

Table 1-2 Symantec Endpoint Encryption protocols and ports

Application layer protocol	Communication protocol	Purpose	Used by	Port
Group Policy Core Protocols	TCP/IP	Deliver and consume Group Policy Objects (GPOs)	Symantec Endpoint Encryption Client Computers Management Console Computers	445, 389
SOAP over Hypertext Transport Protocol (HTTP)	TCP/IP	Communicate between the clients and the server	Symantec Endpoint Encryption Client Computers Symantec Endpoint Encryption Management Server	configurable
JSON over Hypertext Transport Protocol (HTTP)	TCP/IP	Web-based Help Desk Recovery	Symantec Endpoint Encryption Management Server Web browser	Configurable. Ensure that you specify the same port number as JSON over HTTP.

Table 1-2 Symantec Endpoint Encryption protocols and ports *(continued)*

Application layer protocol	Communication protocol	Purpose	Used by	Port
Lightweight Directory Access Protocol (LDAP)	TCP/IP	Query Active Directory and eDirectory directories	Symantec Endpoint Encryption Management Server	389, 3268, or configurable
Tabular Data Stream (TDS)	TCP/IP	Communicate between the server and the database	Symantec Endpoint Encryption Management Server Symantec Endpoint Encryption database Management Console Computers	1433, dynamically allocated, or configurable
Transport Layer Security (TLS) and/or Secure Sockets Layer (SSL)	TCP/IP	Optionally encrypt communications by layering these protocols on top of TDS, LDAP, and/or HTTP	Symantec Endpoint Encryption Management Server Symantec Endpoint Encryption database Management Console Computers Symantec Endpoint Encryption Client Computers	636, 3269, or configurable

Accounts required by Symantec Endpoint Encryption

Symantec Endpoint Encryption requires the following accounts:

Table 1-3 Accounts of Symantec Endpoint Encryption

Account	Description
Database creation account	You must have an account that can access Microsoft SQL Server so that you can install and configure the Symantec Endpoint Encryption Management Server. You can either use a Microsoft Windows domain account or a Microsoft SQL account. If you use a Microsoft Windows domain account, it must have local administrator rights on the Symantec Endpoint Encryption Management Server computer. If you use Microsoft SQL authentication, Symantec Endpoint Encryption uses this account to create and configure the Symantec Endpoint Encryption Management Server database during installation. Symantec Endpoint Encryption does not store the credentials for this Microsoft SQL account. The account login requires the following roles: ■ `public` ■ `sysadmin`

Table 1-3 Accounts of Symantec Endpoint Encryption *(continued)*

Account	Description
Database access account	The database access account is used by the Symantec Endpoint Encryption Services web site (web service) to interact with the Symantec Endpoint Encryption database. The Configuration Manager also uses this account. You can either use Microsoft Windows authentication or Microsoft SQL authentication. Symantec recommends that you use Microsoft Windows authentication for your database access account. If you use Microsoft Windows authentication you must provide an existing Microsoft Windows domain account. It should not be an administrator. It does require privileges on the database, registry, and the file system. If you use Microsoft Windows authentication for database access account, the account is also used as a logon account for the AD Synchronization service. If the login that you specify for your database access account does not exist, the installer creates and configures the login and the corresponding database user. If the login already exists, then you have an option to use it. The installer creates the corresponding database user is created and configured for you by installer. The database access account requires the following database roles: ■ `db_datareader` ■ `db_datawriter` ■ `public` The installer also grants the database access account Execute permission. See "Setting up the rights for the database access account" on page 12.
IIS client authentication account	Each client computer shares a single domain user account. It uses this account for basic authentication to IIS on the Symantec Endpoint Encryption Management Server. The IIS client authentication account is a regular domain user account and does not require specific privileges.
Policy Administrator account	Policy Administrators require read-write access to the Symantec Endpoint Encryption database. You can use either a Microsoft Windows or a Microsoft SQL account. This account lets the Policy Administrator use the snap-ins of the Management Console. If you choose to use a Microsoft Windows account for database access, you can create a Policy Administrators group to make administration easier.

Table 1-3 Accounts of Symantec Endpoint Encryption *(continued)*

Account	Description
Active Directory synchronization account	Synchronization with Active Directory requires a domain account. The Active Directory synchronization service uses this account to bind to Active Directory. You may need to extend the account's privileges to include read permissions to the deleted objects container in Active Directory.

Note: When you install, if you select the option to use an existing database, make sure that the database access account (Windows/SQL) conforms to the roles and permissions that are specified above. If it does not, then you must manually provision the account.

Setting up the rights for the database access account

If you plan to use Microsoft Windows authentication with your SQL Server instance, you must provision a Microsoft Windows domain account before you install the Symantec Endpoint Encryption Management Server. If you use Microsoft SQL authentication, the installer automatically assigns these rights.

See "Accounts required by Symantec Endpoint Encryption" on page 9.

To set up the rights for the database access account:

1. Give the account read and write access to this registry folder:

   `HKLM\Software\Symantec\Endpoint Encryption.`

2. Give the account read and write access to the log directory. By default the log is stored at:

   `C:\Program Files(x86)\Symantec\Symantec Endpoint Encryption Management Server\Services\Logs`

3. Add the Microsoft Windows account in SQL Server login accounts and map it to the Symantec Endpoint Encryption database. It requires the `db_datareader`, `db_datawriter`, and `public` roles on the Symantec Endpoint Encryption database.

4. When you run the installer, in the **Database Configuration** tab you specify the Symantec Endpoint Encryption Management Server account's user name and password for database access through Windows Authentication.

About Symantec's Community Quality Program

Symantec Endpoint Encryption offers the Symantec Community Quality Program. This program submits anonymous system and product information about how you use this product to Symantec. Involvement in the program is optional. You opt in to the program using the Symantec Endpoint Encryption Management Server Configuration Manager.

About the Microsoft SQL Server credential for the Community Quality Program

Microsoft SQL Server credentials are required to support program participation. During an installation or upgrade to Symantec Endpoint Encryption 11.2.0, Symantec Endpoint Encryption creates a Microsoft SQL Server credential. This credential has minimal access to the Symantec Endpoint Encryption database.

The Community Quality Program requires mixed-mode authentication to your Microsoft SQL Server database server.

Detailed information about this credential is as follows:

Element	Access
Logon access	SEEMSDb
Module access	Specific to the Community Quality Program module
User account name	see_telemetry_user **Note:** This credential is used when you opt in to the program. If the account name already exists in Microsoft SQL Server, digits are appended to distinguish individual account names.
EXECUTE access	To the following telemetry stored procedures: ■ Telemetry_AdminActivity ■ Telemetry_BacklogItems ■ Telemetry_ClientDataByOS ■ Telemetry_ClientDataByVer ■ Telemetry_ClientEvent ■ Telemetry_PurgeBacklogItems ■ Telemetry_QueryConfigServer ■ Telemetry_ServerDeployment
SELECT, INSERT, UPDATE, DELETE, ALTER access	To the TelemetryBacklog database table
INSERT access	To the GEMSEventLog database table

About the Community Quality Program in a server cluster environment

The Community Quality Program can operate in a deployment that uses server clusters.

However, within the server cluster, only one of the servers can have the Telemetry module sending statistics to the Symantec Central Telemetry server. That server is the server on which you most recently opted in to the program from the make sure your preference is preserved by launching Configuration Manager on an active Symantec Endpoint Encryption Management Server in the deployment. Configuration Manager.

If you uninstall servers from a cluster, make sure your preference is preserved by launching the Configuration Manager on an active Symantec Endpoint Encryption Management Server.

For more information on the Community Quality Program, see the following:

- For information about the Community Quality Program page in the Symantec Endpoint Encryption Management Server Configuration Manager, see:
  See "Community Quality Program page" on page 101.
- For information about troubleshooting telemetry settings, see:
  http://www.symantec.com/docs/HOWTO110233

Best practices for Microsoft SQL Server database logons

Symantec recommends the following best practices for Microsoft SQL Server database logons:

- Create and use an Active Directory account for Microsoft SQL authentication (do not use SQL Server credentials).
- Restrict access on the Microsoft SQL Server database to the minimum number of users that require access to the Management Console.
- Computers where you install the Management Console should run an industry standard security profile.

Roles required by Symantec Endpoint Encryption

Symantec Endpoint Encryption requires the following roles:

The policy administrator role

The policy administrator uses the Management Console for centralized administration of Symantec Endpoint Encryption.

Policy administrators use a Microsoft Windows account to log on to their computer. Microsoft Windows and Microsoft SQL Server maintain the policy administrator's account privileges. Symantec Endpoint Encryption does not manage these accounts. You can use Microsoft

Windows privileges to restrict access to snap-ins of the Management Console to specific policy administrators.

Policy administrators require access privileges to the Symantec Endpoint Encryption database.

Policy administrators can do the following:

- Update and set client policies.
- Issue the commands to encrypt or decrypt the client computers.
- Run the reports.
- Change the Management Password.
- Run the Help Desk Recovery.

The client administrator role

Client administrators provide local support to Symantec Endpoint Encryption users.

You manage client administrator accounts from the Management Console. Symantec Endpoint Encryption manages the client administrator accounts. It manages them independent of operating system or directory service so that client administrators can support a wide range of users. Client administrators authenticate with a password. You manage the password from the Management Console. This single-source password management lets your client administrators remember only one password as they move among many client computers.

Client computers must have one default client administrator account. Client administrators can perform hard disk recovery. You can have up to 1024 total client administrator accounts on a client computer. These client administrators are counted separately from the 1024 registered users. If a policy has more 1024 client administrators, the client registers only the first 1024 client administrators in the policy.

Client administrators can always authenticate to client computers and can always initiate encryption. You should trust client administrators according to their assigned level of privilege.

The user role

Drive Encryption protects the data on the client computer. It requires valid credentials before it allows the operating system to load. Users set their Symantec Endpoint Encryption credentials. The credentials let them power on the computer access to the operating system. Drive Encryption only accepts the credentials of registered users and client administrators.

The client requires at least one user to register with Symantec Endpoint Encryption. You can configure the registration process to occur without user intervention. When you create an installation package, you can allow up to a maximum of 1024 users per computer. You can manage your users through policies.

Do not define users as local administrators or give users local administrative privileges.

About the Management Password

The Management Password is an important part of installing and upgrading Symantec Endpoint Encryption. If you do not already have a Management Password, you are prompted to create one when you install Symantec Endpoint Encryption Management Server 11.2.0 for the first time. When you set the Management Password, it is encrypted and stored in the Symantec Endpoint Encryption database. You can change the Management Password at any time after installation, in the Management Console.

You are required to enter the Management Password to:

- Install and upgrade Symantec Endpoint Encryption Management Server
- Install and upgrade the Management Console
- Access the Help Desk Recovery snap-in in the Management Console
- Create the Autologon Utility installation package
- Create the Windows Password Reset Utility installation package

Do not lose your Management Password. Symantec cannot recover this password if it is lost. If you lose your Management Password you must reinstall the Management Server.

Symantec recommends that you protect and store your Management Password in a safe location. You should establish a protocol within your organization for all Management Password changes. Use this protocol to prevent situations where multiple administrators could inadvertently change the Management Password and prevent other administrators from accessing the functions that they require.

Symantec Endpoint Encryption Microsoft SQL Server Feature Pack requirements

- Microsoft System CLR Types version 10.3.5500.0 or later for SQL Server 2008 (32-bit)
- Microsoft SQL Server 2008 (32-bit) Management Objects version 10.3.5500.0 or later

---

Note: You require these pre-requisites only when you upgrade the Management Console on a Windows Server computer.

Download the Microsoft SQL Server Feature Pack from:

https://www.microsoft.com/en-in/download/details.aspx?id=26728

Enabling the prerequisite server roles, features, and tools for the Symantec Endpoint Encryption Management Server

You must enable the prerequisite server roles, features, and tools to install Symantec Endpoint Encryption. Do not attempt to install until you complete the steps in this topic.

On Microsoft Windows Server 2016

To enable the Web service (IIS) role on a Microsoft Windows 2016 Server:

1. Go to **Start > Programs > Administrative Tools > Server Manager**.
2. In the **Dashboard**, click **Add roles and features**.
3. In the **Add Roles and Features Wizard**, click **Next**.
4. In the **Installation Type** page, click **Role-based or feature-based installation** and then click **Next**.
5. In the **Server Selection** page, make the selection that matches your environment and then choose your server and click **Next**.
6. In the **Server Roles** page, select **Web Server (IIS)**.
7. In the **Add Roles and Features Wizard** window, click **Include management tools** and then click **Add Features**.
8. Click **Next**.
9. In the **Features** page, expand **.NET Framework 4.6 Features** and check **.NET Framework 4.6** and **ASP.NET 4.6**.
10. In the **Features** page, check **Group Policy Management**.
11. In the **Features** page, expand **Remote Server Administration Tools > Role Administration Tools** and check **AD DS and AD LDS Tools**.
12. Click **Next**.
13. In the **Web Server Role (IIS)** page, click **Next**.
14. In the **Role Services** page, expand **Web Server > Security** and select **Basic Authentication** and **Windows Authentication**.
15. In the **Role Services** page, expand **Web Server > Application Development** and check the following:
    - **.NET Extensibility 4.6**
    - **ASP .NET 4.6**
    - **ISAPI Extensions**

- **ISAPI Filters**

16 In the **Role Services** page, expand **Management Tools** and check the following:

- **IIS Management Console**
- **IIS 6 Management Compatibility** (check all four entries)
- **IIS Management Scripts and Tools**

17 Click **Next**.

18 In the **Confirmation** page, click **Install**.

19 In the **Results page**, click **Close**.

On Microsoft Windows Server 2012

To enable the Web service (IIS) role on a Microsoft Windows 2012 Server:

1 Go to **Start > Programs > Administrative Tools > Server Manager**.

2 In the **Dashboard**, click **Add roles and features**.

3 In the **Add Roles and Features Wizard**, click **Next**.

4 In the **Installation Type** page, click **Role-based or feature-based installation** and then click **Next**.

5 In the **Server Selection** page, make the selection that matches your environment and then choose your server and click **Next**.

6 In the **Server Roles** page, select **Web Server (IIS)**.

7 In the **Add Roles and Features Wizard** window, click **Include management tools** and then click **Add Features**.

8 Click **Next**.

9 In the **Features** page, expand **.NET Framework 4.5 Features** and check **.NET Framework 4.5** and **ASP.NET 4.5**.

10 In the **Features** page, check **Group Policy Management**.

11 In the **Features** page, expand **Remote Server Administration Tools > Role Administration Tools** and check **AD DS and AD LDS Tools**.

12 Click **Next**.

13 In the **Web Server Role (IIS)** page, click **Next**.

14 In the **Role Services** page, expand **Web Server > Security** and select **Basic Authentication** and **Windows Authentication**.

15 In the **Role Services** page, expand **Web Server > Application Development** and check the following:

- **.NET Extensibility 4.5**
- **ASP .NET 4.5**
- **ISAPI Extensions**
- **ISAPI Filters**

16 In the **Role Services** page, expand **Management Tools** and check the following:

- **IIS Management Console**
- **IIS 6 Management Compatibility** (check all four entries)
- **IIS Management Scripts and Tools**

17 Click **Next**.

18 In the **Confirmation** page, click **Install**.

19 In the **Results page**, click **Close**.

On Microsoft Windows Server 2008

To enable the web server (IIS) server role and role services on Microsoft Windows Server 2008:

1 Click **Start > Administrative Tools > Server Manager**.

2 In the left pane of the **Server Manager** snap-in, right-click **Roles** and click **Add roles**.

3 On the welcome page of the **Add Roles Wizard**, click **Next**.

4 On the **Select Server Roles** page, select **Web Server (IIS)**.

5 Click **Next** and then click **Next** again.

6 On the **Select Role Services** page, go to **Web Server > Application Development** and click **ASP.NET**.

7 On the **Add role services and features required for ASP.NET** dialog box, click **Add Required Role Services**. Selecting this option also automatically selects **.NET Extensibility**, **ISAPI Extensions**, and **ISAPI Filters**.

8 Expand the **Security** option and then click **Basic Authentication** and **Windows Authentication**.

9 Expand **Management Tools** and check **IIS Management Scripts and Tools**. Check **IIS 6 Management Compatibility**. Make sure all the components under **Management Compatibility** are also checked.

10 Click **Next** and then click **Install**.

11 After the **Add Roles Wizard** indicates that the installation is successful, click **Close**.

12 In the left pane of the **Server Manager** snap-in, right-click **Features** and click **Add features**.

13 In the **Select Features** window, select **.NET Framework 4.5 features**.

14 Select **Group Policy Management**.

15 Expand **Remote Server Administration Tools > Role Administration Tools** and select **AD DS and AD LDS Tools**.

16 Click **Next** and then click **Install**.

17 After the **Add Roles Wizard** indicates that the installation is successful, click **Close**.

About configuring TLS/SSL communications for Symantec Endpoint Encryption

Symantec Endpoint Encryption supports secure communications using TLS/SSL. The specifics of how you have set up TLS/SSL are dependent on your specific environment. This section assumes that you are familiar with how your organization has implemented TLS/SSL. This section lists the requirements that Symantec Endpoint Encryption has for TLS/SSL communications in addition to your unique implementation.

About securing communications between the Symantec Endpoint Encryption Management Server and client computers

You can use TLS/SSL communications to secure the traffic between your client computers and the Symantec Endpoint Encryption Management Server. To use TLS/SSL, you must provide a server-side TLS/SSL certificate on the Symantec Endpoint Encryption Management Server. You must also provide a client-side CA certificate when you install the Symantec Endpoint Encryption Management Server.

The server-side TLS/SSL certificate must comply with the following requirements:

- It must be valid for IIS.
- It must be valid during the period in which you use it.
- You must enable it for server authentication.
- It must contain a private key.
- The common name (CN) must match the name of the Symantec Endpoint Encryption Management Server exactly. You set this value it in the **Web Server Name** field of the **Configuration Wizard** or the **Configuration Manager**.
- The same certificate authority that issued the client-side CA certificate must also issue the server-side certificate.
- You must install it in the local computer personal certificate store of the Symantec Endpoint Encryption Management Server.

The client-side CA certificate must comply with the following requirements:

- It must be in the .CER file format.
- It must be valid during the period in which you use it.
- It must be the root certificate of the same certificate authority that issued your server-side TLS/SSL certificate.

About securing communications between the Symantec Endpoint Encryption Management Server and the database

You can use TLS/SSL communications to secure the traffic between your Symantec Endpoint Encryption database and the Symantec Endpoint Encryption Management Server. To use TLS/SSL, you must provide a server-side TLS/SSL certificate on the Symantec Endpoint Encryption Management Server. You must also provide a client-side CA certificate when you install the Symantec Endpoint Encryption Management Server

You use the SQL Server Configuration Manager snap-in to enable SSL encryption and to assign the TLS/SSL certificate.

If the server hosting the Symantec Endpoint Encryption database is not a domain member, you must issue the TLS/SSL certificate to the NetBIOS name. You must also install it in the personal certificate store of the computer that hosts the Symantec Endpoint Encryption database.

The server-side TLS/SSL certificate must comply with the following requirements:

- It must be valid during the period in which you use it.
- You must enable it for server authentication.
- If the server is a member of the domain, the certificate must contain a private key. The private key must be issued to the FQDN of the server that hosts the Symantec Endpoint Encryption database.

Using TLS 1.2 with Mac OS clients running FileVault 2

The Symantec Endpoint Encryption Management Server supports TLS 1.2 secure communications with Mac OS clients running FileVault 2.

Specifics of this functionality are:

- Mac clients with FileVault 2 enabled can connect to the Symantec Endpoint Encryption Management Server using only TLS 1.2.
- When clients connect that are running previous versions of Symantec Endpoint Encryption, the server continues to support TLS 1.0 for backward compatibility.

About securing communications between Symantec Endpoint Encryption Management Server and Active Directory

You can use TLS/SSL communications to secure the traffic between your Active Directory and the Symantec Endpoint Encryption Management Server. To use TLS/SSL, you must provide a server-side TLS/SSL certificate on the domain controller.

This certificate must comply with the following requirements:

- It must be valid during the period in which you use it.
- You must enable it for server authentication.
- It must contain the private key of the domain controller's FQDN. This key is from the Personal certificate store on the computer that hosts the domain controller.

Best practices for configuring encrypted communications

When configuring encrypted communications, consider the following best practices:

- Make sure that the SQL Server CA certificate is present in trusted root cert store.
- Use the common name (CN) string from the server certificate as the **Database server name**. The **Database server name** is required in the Installation Wizards of the Symantec Endpoint Encryption Management Server, Management Console, and the **Database config** tab in the **Configuration Manager**.
- The common name (CN) string should appear as a FQDN. You should be able to resolve its IP address using DNS lookup or hosts file lookup.

Installing prerequisite software on your Management Console

The Management Console requires the Remote Server Administration Tools, and it also requires the .NET framework.

Microsoft SQL Server Feature Pack should be installed on a server class system (Windows Server 2012 R2 and Windows Server 2008 R2) before installing the Management Console.

See “Symantec Endpoint Encryption Microsoft SQL Server Feature Pack requirements” on page 16.

Setting up the Remote Server Administration Tools

You must set up the Remote Server Administration Tools before you install the Management Console.

To set up the Remote Server administration Tools on Microsoft Windows Server 2012:

- Follow the instructions to enable Microsoft Remote Server Administration Tools for Microsoft Server 2012 at

  http://social.technet.microsoft.com/wiki/contents/articles/2202.remote-server-administration-tools-rsat-for-windows-client-and-windows-server-dsforum2wiki.aspx

To set up the Remote Server Administration Tools on Microsoft Windows Server 2008 R2

- Follow the instructions to enable Microsoft Remote Server Administration Tools for Microsoft Server 2008 at:

  http://technet.microsoft.com/en-us/library/cc816817%28v=ws.10%29.aspx

To set up the Remote Server Administration Tools on Microsoft Windows 8:

- Download and install the Microsoft Remote Server Administration Tools for Microsoft Windows 8 from:

  http://www.microsoft.com/en-us/download/details.aspx?id=28972

To set up the Remote Server Administration Tools on Microsoft Windows 7:

- Download and install the Microsoft Remote Server Administration Tools for Microsoft Windows 7 from:

  http://www.microsoft.com/downloads/details.aspx?FamilyID=7D2F6AD7-656B-4313-A005-4E344E43997D&displaylang=en

Chapter 2

Upgrading Symantec Endpoint Encryption Management Server

This chapter includes the following topics:

About upgrading from previous releases

There are two ways to upgrade your Symantec Endpoint Encryption Management Server. You can either upgrade in-place to the latest version or you can do a side-by-side migration.

In-place upgrade	An in-place upgrade means that you upgrade the Symantec Endpoint Encryption Management Server components to the latest version without uninstalling the current version. Note that previous client versions can still communicate with Symantec Endpoint Encryption Management Server 11.2.0. Symantec Endpoint Encryption Management Server 11.2.0 supports an in-place upgrade for the following versions: ■ Symantec Endpoint Encryption 8.2.1 and later Maintenance Packs ■ Symantec Endpoint Encryption 11.0.0 MP3 ■ Symantec Endpoint Encryption 11.0.1 MP1 ■ Symantec Endpoint Encryption 11.1.0 ■ Symantec Endpoint Encryption 11.1.1
A side-by-side migration	A side-by-side migration means that you install new management components on new hardware and you leave the previous version's installation as is. Over time, you can gradually migrate your clients to report to the new Symantec Endpoint Encryption Management Server as you upgrade them.

Backward compatibility

The following previous versions of Symantec encryption client products are compatible with Symantec Endpoint Encryption Management Server 11.2.0:

- Symantec Endpoint Encryption 8.2.1 and later Maintenance Packs
- Symantec Endpoint Encryption 11.0.0 MP3
- Symantec Endpoint Encryption 11.0.1 MP1
- Symantec Endpoint Encryption 11.1.0
- Symantec Endpoint Encryption 11.1.1

Note: You can configure Symantec Endpoint Encryption Management Server 11.2.0 to connect to Symantec Encryption Management Server 3.3.2 MP1 or later to obtain recovery tokens for Symantec Encryption Desktop clients (version 10.3.2 MP1 or later). However, you cannot use Symantec Endpoint Encryption Management Server 11.2.0 to manage Symantec Encryption Desktop clients.

Symantec Endpoint Encryption Drive Encryption features compatibility

After you upgrade to Symantec Endpoint Encryption 11.2.0, the following Drive Encryption features are available in earlier versions of Symantec Endpoint Encryption clients:

Decryption and encryption using server commands

You can use server commands available in Symantec Endpoint Encryption 11.2.0 to encrypt and decrypt disks as well as the disk partitions that you previously managed using earlier versions of Symantec Endpoint Encryption.

For example, if you deployed Symantec Endpoint Encryption Full Disk but did not encrypt the disk, and then you upgraded to Symantec Endpoint Encryption 11.2.0, you can still encrypt the disk. You can do this using the encryption and decryption server commands that are available in Symantec Endpoint Encryption 11.2.0. You can also decrypt a disk that was encrypted using earlier versions of Symantec Endpoint Encryption clients.

The server commands that are available in Symantec Endpoint Encryption 11.2.0 are not backward-compatible with the clients of Symantec Endpoint Encryption Management Server 8.0.1 SP4 and GuardianEdge Management Server 9.5.3.SP3.

Authentication

You can enable user authentication on earlier versions of Symantec Endpoint Encryption using passwords, tokens, or both methods.

Recovery

In earlier version of Symantec Endpoint Encryption, the One-Time Password (OTP) policy (now referred to as Help Desk Recovery) and the Authenti-Check policy (now referred to as Self-Recovery) were user policies. In Symantec Endpoint Encryption Management Server 11.2.0, you configure these policies as computer policies.

When you upgrade to Symantec Endpoint Encryption 11.2.0, you can still create Self-Recovery and One-Time Password user policies using Group Policy Objects. Also, users can use the Help Desk Recovery tokens that were generated using Symantec Endpoint Encryption 11.2.0 to unlock and authenticate users on earlier versions of Symantec Endpoint Encryption clients.

Client Administrators

You can create client administrator accounts on earlier versions of Symantec Endpoint Encryption server as well as manage them. You can add additional client administrators on your earlier versions of Drive Encryption clients, if there are less than 1024 client administrators.

After you upgrade to Symantec Endpoint Encryption 11.2.0, you cannot configure the administrative privileges and authentication method that is associated with a client administrator account. Therefore, any client administrator account that you create after you upgrade has all the administrative privileges and authenticates using a password by default.

Note: After you upgrade to Symantec Endpoint Encryption 11.2.0, ensure that you change all of the client administrator passwords.

Reports and logs

You can generate reports to view information such as client version, user information, and encryption and decryption status of disks or files on the client computers. You use the new

report template that is available in Symantec Endpoint Encryption 11.2.0. You can also monitor event logs for creating or modifying a client administrator, server commands, and policy updates to your previous versions of Symantec Endpoint Encryption clients.

Symantec Endpoint Encryption Removable Media Access Utility features compatibility

The Removable Media Access Utility is now available as a part of Removable Media Encryption. You can access a file encrypted with earlier versions of Symantec Endpoint Encryption 11.2.0 using Removable Storage. However, on a managed computer running Removable Media Encryption 11.2.0, you cannot use Removable Media Access Utility to edit, copy, paste, and drag and drop files or folders to a device. After you upgrade to Symantec Endpoint Encryption 11.2.0, you cannot encrypt a file on previous versions of Symantec Endpoint Encryption using Removable Media Access Utility.

Deprecated policy options

After you upgrade to Symantec Endpoint Encryption11.2.0, and create a new policy, the deprecated policy options from earlier versions are reset to their default settings and can no longer be modified. Therefore, when you upgrade to Symantec Endpoint Encryption 11.2.0, be sure to review the settings that are configured for each policy.

For more information, see www.symantec.com/docs/TECH224469.

About creating 8.2.1 installation packages in Symantec Endpoint Encryption 11.2.0

You can create Symantec Endpoint Encryption 8.2.1 (with MP16 version) installation packages in a Symantec Endpoint Encryption 11.2.0 environment. This feature lets you continue to deploy, reinstall, or change the install-time policies of 8.2.1 (with MP16 version) clients.

You can create the MP16 version of installation packages for Symantec Endpoint Encryption 8.2.1 in a Symantec Endpoint Encryption 11.2.0 environment. This ability lets you continue to deploy, reinstall, or change the install-time policies of your clients that are running the MP16 version of 8.21. These clients can include clients running on older operating systems such as Microsoft Windows XP.

To create 8.2.1 client installation packages, you use a dedicated Symantec Endpoint Encryption 8.2.1 Management Console. This console is not part of the Symantec Endpoint Encryption 11.2.0. It is kept at 8.2.1 MP16 and used to generate client installers that are applied to client computers running the MP16 version of 8.2.1.

When you upgrade to Symantec Endpoint Encryption 11.2.0, you upgrade the database and the Symantec Endpoint Encryption Management Server and install a new Management Console. This is done independently of keeping a dedicated 8.2.1 Management Console. You complete all of your remaining management tasks and reporting tasks from the new Management Console 11.2.0.

Note: Symantec Endpoint Encryption 11.2.0 only supports creating 8.2.1 installation packages with MP16 version.

If you are not running version 8.2.1 with the MP16 version, you must first upgrade to the Maintenance Pack16 before you can take advantage of this feature.

Upgrading the server

To upgrade your Symantec Endpoint Encryption Management Server from a previous release, complete the following tasks:

Note: If you plan to use dual console versions to create 8.2.1 installation packages in Symantec Endpoint Encryption 11.2.0, you must first migrate to version 8.2.1 MP16.

See "About creating 8.2.1 installation packages in Symantec Endpoint Encryption 11.2.0" on page 27.

Table 2-1 Process for Upgrading your Symantec Endpoint Encryption Management Server

Action	Description
Meet the minimum system requirements	Do the following: ■ Make sure that the Symantec Endpoint Encryption Management Server's computer meets the minimum system requirements. ■ Make sure that the Symantec Endpoint Encryption database's server meets the minimum system requirements before you install the Symantec Endpoint Encryption Management Server. ■ Make sure that the Management Console computer meets the minimum system requirements. ■ Make sure that the Microsoft SQL Server Feature Pack is installed on a server class system before you install the Symantec Endpoint Encryption Management Server or Management Console. See "Symantec Endpoint Encryption Microsoft SQL Server Feature Pack requirements" on page 16.
Meet the prerequisite services requirements	Verify that IIS is installed and enable the web server (IIS) server role and the required role services. See "Enabling the prerequisite server roles, features, and tools for the Symantec Endpoint Encryption Management Server" on page 17.

Table 2-1 Process for Upgrading your Symantec Endpoint Encryption Management Server *(continued)*

Action	Description
Set up encrypted communications	If you plan to use TLS/SSL encryption for your server communications, you must make sure that the computer meets the prerequisites. ■ To encrypt the communication between the Symantec Endpoint Encryption Management Server and client computers, you must install a TLS/SSL certificate on the Symantec Endpoint Encryption Management Server. You must provide a client-side CA certificate. ■ To encrypt the communication between the Symantec Endpoint Encryption Management Server and the database, you must install a server-side TLS/SSL certificate on the server that hosts the Symantec Endpoint Encryption database ■ To encrypt the directory synchronization traffic, you must install a server-side TLS/SSL certificate on the domain controller. See "About configuring TLS/SSL communications for Symantec Endpoint Encryption" on page 20.
Run the upgrade wizard	Run the upgrade wizard to specify your settings for the server. See the section called " Upgrading the server" on page 29.
Configure the Server.	You use the configuration wizard to set up your directory service synchronization and to configure the Web service. See "Configuring the server" on page 33.
Restart the server	After you finish the steps, restart the computer.
Complete the upgrade	After finishing the Upgrade Wizard and the Configuration Wizard, verify that you set up the server and database correctly and then schedule recurring back ups of the database. See "Completing the upgrade" on page 42.

Upgrading the server

To upgrade the Symantec Endpoint Encryption Management Server, you run the Symantec Endpoint Encryption Suite Installation Wizard and then follow the steps to configure your upgrade settings.

To upgrade the server

1 Do one of the following:

- If your database creation account is a Microsoft Windows account, log on to the server using the account that you used to create the database. The account must have local administrator rights.

- If your database creation account is a Microsoft SQL account, log on to the server using a Microsoft Windows domain account. The account must have local administrator rights.

2 Close all instances of the Microsoft Management Console. The wizard cannot complete if the console is open.

3 Copy the `SEE Server Suite x64.msi` file to the local hard disk of the Symantec Endpoint Encryption Management Server.

4 Do one of the following:

- Double-click the file to run it.
- Use the command line to run the file as follows:

  Click **Start > All Programs > Accessories**. Right-click **Command Prompt**, and then click **Run as administrator**.

  In the command prompt window, run the following command:

  ```
  MSIEXEC /I "[path]\SEE Server Suite x64.msi" /lvx "[logpath]\logfile"
  ```

  `[logpath]` and `\logfile` represent the path and name of the output log file.

5 On the **Welcome** page of the wizard, click **Next**.

6 In the **Symantec Endpoint Encryption Multi-Factor Authentication** page, click **Next**.

7 In the **License agreement** page, select **I accept the terms in the license agreement** and click **Next**.

8 On the **Setup Type** page, you can either accept the default feature set, or choose the features that you want to enable including:

- Management Server
- Management Agent
  - Drive Encryption
  - Removable Media Encryption

Note: When you select **Management Agent**, the SEE Help Desk, Symantec Endpoint Encryption for BitLocker, and Symantec Endpoint Encryption for FileVault features are installed or upgraded by default.

Do one of the following:

- (Default) To enable all of the features, click **Complete**.

Note: When you click **Complete** during an upgrade, the already installed Symantec Endpoint Encryption features are removed. And all the Symantec Endpoint Encryption features are installed on the same system.

- To enable specific features, click **Custom**. and then configure the following options for each feature:

Note: When you click **Custom** during an upgrade, the already installed Symantec Endpoint Encryption features are removed. And only the selected Symantec Endpoint Encryption features are installed.

Feature navigation tree	Lets you control how the features are installed. Click the icon that is next to the feature that you want to change and then select from the following: ■ **This feature will be installed on the local hard drive** ■ **This feature, and all sub-features, will be installed on the local hard drive** ■ **This feature will not be available**
Disk Usage	Lets you view the disk space that is required for the features. Select the feature that you want to view and then click **Disk Usage**.

9 In the **Custom Setup** page, click **Next**.

10 On the **Database Location and Credentials** page, in the **Database Instance** field, provide the location of the database. Symantec recommends that you use a dedicated server for your Symantec Endpoint Encryption database. However, you can install the database locally if you install a supported version of Microsoft SQL Server. You must provide an account for communications between the Symantec Endpoint Encryption Management Server and the Symantec Endpoint Encryption database. Use one of the following methods to either provide a Microsoft SQL account or a Microsoft Windows account.

Click the drop-down menu	Lets you select from a list of local instances.
Click **Browse**	Lets you select from a list of instances on the network,
Enter the NetBIOS name	Lets you type the name of an instance. If you use a named instance, you must also include the name of the instance. For example, **SEEDB-01\NAMEDINSTANCE**.

11 To encrypt communication between the server and the database, click **Enable TLS/SSL**.

To use this feature, you must meet additional prerequisites.

See "About configuring TLS/SSL communications for Symantec Endpoint Encryption" on page 20.

12 If your database server is configured to use a custom port, select **Custom port number** and enter the port number.

13 You must specify the authentication method of your database creation account. Symantec Endpoint Encryption uses this account for communication between the server and the database.

Use the database creation account that you set up in your previous version of Symantec Endpoint Encryption.

To specify the database creation account, select one of the following options:

Windows authentication	This option lets you use the Microsoft Windows domain account that you are currently logged on with. This account has the following characteristic: ■ It has permission to the IIS metabase and file system. The wizard automatically applies the required database permissions and roles to this account.
SQL authentication	This option lets you use a Microsoft SQL Server account. See "Best practices for Microsoft SQL Server database logons" on page 14.

14 Click **Next**.

15 On the **SEE Management Password** page, do the following:

- Provide the Management Password that was set when you first installed your previous version's server.

Warning: Do not lose your Management Password.

Symantec cannot recover this password if you lose it. If you lose your Management Password you must reinstall the Management Server.

Symantec recommends that you protect and store your Management Password in a safe location.

See "About the Management Password" on page 16.

16 Click **Next**.

17 If the **Database Access** page is displayed, enter your credentials for the Symantec Endpoint Encryption database in the **User name** and **Password** fields, and then click **Next**.

18 On the **Ready to Install the Program** page, click **Install**.

19 On the **Installation Wizard Completed** page, click **Finish**.

After the program is installed, the Symantec Endpoint Encryption Management Server Configuration Wizard automatically launches.

See "Configuring the server" on page 33.

Configuring the server

After you run the Symantec Endpoint Encryption Management Server wizard, the configuration wizard automatically launches. You use the wizard to set up your directory service synchronization and to configure the Web service. You can also manually start the wizard by running the configuration manager program on the Symantec Endpoint Encryption Management Server. You must complete the wizard before you can synchronize your directory services and create your client installation packages. You can use the configuration manager to change these settings later.

You use the wizard to complete the following tasks:

Configure the Web service	You use the wizard to configure the communications between the Symantec Endpoint Encryption Management Server and the client computers. You set the protocol and the port that you use for communication. If you intend to use SSL, then you must also provide the communication certificates.
Specify the directory service	Directory service synchronization lets you keep the database current with the information in your directory services. For example, when computers are added and removed from Active Directory, the server synchronizes those changes with the Symantec Endpoint Encryption database. This synchronization lets you use the Management Console to apply policies according to your organization's directory Organizational Units and containers. **Note:** In Symantec Endpoint Encryption 11.2.0, the default startup mode of Novell synchronization service is set as manual and the service is stopped by default. If any Novell configuration data exists in a referenced Symantec Endpoint Encryption database, then the startup mode of Novell synchronization service is set as automatic and the service starts, as in Symantec Endpoint Encryption versions earlier than 11.0. See "About configuring TLS/SSL communications for Symantec Endpoint Encryption" on page 20.

Configure directory service synchronization	If you choose to synchronize your directory service, the **Directory Service Synchronization Configuration** page is displayed. Use this page to enter the configuration details about your Active Directory forests. You can add additional forests, and you can exclude domains from synchronization. If you selected the **Microsoft Active Directory** check box on the **Directory Service Synchronization Options** page, the **Active Directory Configuration** area is available. If you select the Novell **eDirectory** check box on the **Directory Service Synchronization Options** page, the **Novell Configuration** area is enabled for editing.

To configure the server

1 In the **Web Service Configuration** dialog box, in the **Web Server Name** field, enter the name of the web server.

The name is pre-filled with the NetBIOS name of the computer that hosts the Symantec Endpoint Encryption Management Server.

If you want to use HTTPS communication between the server and the client computers, this name must match the common name (CN). You specify the common name (CN) in the server-side TLS/SSL certificate.

You must modify this field to include the fully qualified domain name (FQDN) under the following circumstance:

If DNS configuration issues prevent the NetBIOS name from resolving, an FQDN is more appropriate for your network environment.

2 In the **Credentials** section, enter the credentials and domain of the IIS client account.

These fields display the name and domain of the Internet Information Services (IIS) client account. If you change the IIS client account, you must enter the credentials for this account.

- **User name**
  Enter the user name for the IIS client account.
- **Password**
  Enter the password for the IIS client account.
- **Show password**
  Select this option to display the characters that you type in the **Password** field.
- **Enable Windows Authentication**

Select this option to distribute a Removable Media Encryption workgroup key to your Active Directory computers. To enable Windows authentication, the Windows authentication server role must be selected from the **Add Roles and Feature Wizard**. When you use an alias for Symantec Endpoint Encryption Management Server with Windows Authentication enabled, add the alias name as the Service Principal Name for the server computer in Active Directory. This action ensures successful client-server communication. Refer to the Microsoft documentation for adding the alias name as the Service Principal Name.

After you save your changes, the dialog displays the message, "**Changes are saved successfully**." The password characters are obfuscated with symbols.

3 In the **Protocol** section, do one of the following:

To use HTTP communications	If you do not want to encrypt client communications with the Symantec Endpoint Encryption Management Server, click **HTTP**. In the **HTTP port** field enter the number of the TCP port on the Symantec Endpoint Encryption Management Server to use for the unencrypted client communications. By default, the port is 80.
To use HTTPS communications	To encrypt client communications with the Symantec Endpoint Encryption Management Server, click **HTTPS**. In the **HTTPS port** field, enter the TCP port on the Symantec Endpoint Encryption Management Server to use for the encrypted client communications. By default, the port is 443. The wizard requires a TCP port for unencrypted communication even if you use HTTPS. IIS requires this information, but Symantec Endpoint Encryption does not use this port.

4 (If using HTTPS) In the **Client Computer Communications** section, next to the **Client-Side CA Certificate** field, click **Browse**.

5 In the **Choose SSL certificate file** dialog box, the available certificates are displayed from the personal certificate store of the local computer. Select the client-side CA certificate that the client computers use for encrypted communication with the server, and click **Open**.

After you click **Open**, the dialog box should display the certificate hash string under the **Browse** button.

6 (If using HTTPS) In the **Client Computer Communications** section, next to the **Server-Side TLS/SSL Certificate** field, click **Browse**.

7 In the **Certificate selection** dialog box, the available certificates are displayed from the personal certificate store of the local computer. Select the server-side TLS/SSL certificate that the server's Web service uses, and click **OK**.

After you click **OK**, the dialog box should display the certificate hash string under the **Browse** button.

When you select the certificate, you also assign it to the Symantec Endpoint Encryption Services website through the IIS Manager snap-in.

8 In the wizard, click **Next**.

9 On the **Directory Configuration** page, in the **Active Directory Forest Name** field, enter the name of the Active Directory forest that you want to configure.

10 In the **Preferred Global Catalog Server** field, enter the Fully Qualified Domain Name (FQDN) of a global catalog server for the forest.

11 In the **Active Directory User Name**, **Password**, and **Confirm Password** fields, enter the credentials of the Active Directory synchronization account.

12 In the **User Domain** field, enter the NetBIOS name of the Active Directory synchronization account.

13 To encrypt all synchronization traffic between Active Directory and the Symantec Endpoint Encryption Management Server, click **Enable TLS/SSL** . Make sure that you are in compliance with the prerequisites.

14 To exclude Active Directory domains from synchronization, click **Configure Domain Filter**.

For example, there may be domains within your forests that do not contain Symantec Endpoint Encryption client computers. To improve performance and usability, you can exclude these domains from being synchronization.

15 In the **Include Computers from** column on the left, select a domain that you want to exclude.

16 To move a domain into the **Exclude Computers from** column, click **>**.

When you exclude a parent domain, you also exclude all of the child domains of that domain. In a typical deployment, you can first exclude the top level of the domain. You can then only choose to include the child domains that contain the Symantec Endpoint Encryption client computers.

17 Click **OK**.

18 To synchronize with additional Active Directory forests, click **Add**.

The status text on the top-right side of the **Active Directory Forest Name** field updates to display the number of this forest and the new total number of forests.

For example, **2/2 AD Forest** indicates that the wizard displays the configuration settings for the second of a total of two forests. Enter the configuration information for the additional forest.

19 To remove the configuration information for the currently displayed forest, click **Delete**.

20 To view the configuration information for the previous forest, click **Prev**.

21 In the **Novell Tree Name** field, enter the name of the specified tree.

22 In the **LDAP Host Server IP** field, and the **LDAP Port** field, enter the IP address and port of the eDirectory host for the specified tree.

23 (Optional). In the **User Distinguished Name**, **Password**, and **Confirm Password** fields, you can provide the distinguished name (DN) and password of the Novell synchronization account.

24 (Optional) To synchronize with additional eDirectory trees, click **Add**. You can then enter the configuration information for the new tree. The status text above the right side of the Novell Tree Name field updates to display that you have multiple trees. For example, **2/2 Novell Tree**.

25 Click **Next**.

26 On the **Directory Synchronization** page, to synchronize your directory service, click **Activate Directory Synchronization**.

27 Configure the following Synchronization Settings:

Method	This section lets you to control whether the synchronization service runs automatically when Windows starts. If you want the service to run automatically and synchronize at boot time, choose **Automatic synchronization**. If you do not want the service to run automatically and synchronize at boot time, choose **On-demand synchronization**.
Server Type	To control whether this server should act as a primary synchronizer or a secondary synchronizer, use this section. If you plan to deploy only one Symantec Endpoint Encryption Management Server, the server automatically synchronizes with the directory services. It synchronizes regardless of whether you configure it to act as a primary synchronizer or a secondary synchronizer. Choose either **Primary synchronizer** or **Secondary synchronizer**.

28 Click **Finish**.

29 Click **Restart** if prompted.

Upgrading a Management Console

To install and upgrade the Management Console, you run the Symantec Endpoint Encryption Suite Installation Wizard and then follow the steps to configure your installation settings. In the wizard, you must indicate if you use token authentication in your environment, and how the Management Console is to connect to the Symantec Endpoint Encryption database.

To Upgrade a Management Console:

1 Use your Policy Administrator account to log on to the computer where you want the Management Console.

See "Accounts required by Symantec Endpoint Encryption" on page 9.

2 Close all instances of the Microsoft Management Console. The wizard cannot complete if the console is open.

3 Copy the `<filename>` file to the local hard disk of the Management Console, where the <filename> is one of the following:

- If the Management Console computer's operating system is 32-bit: `SEE Server Suite.msi`
- If the Management Console computer's operating system is 64-bit: `SEE Server Suite x64.msi`

4 Do one of the following:

- Double-click the file to run it.
- Use the command line to run the file as follows:
  Click **Start > All Programs > Accessories**. Right-click **Command Prompt**, and then click **Run as administrator**.
  If you are prompted, enter the credentials of a domain administrator account.
  In the command prompt window, run the following command:
  `MSIEXEC /I "[path]\<filename>" /lvx "[logpath]\logfile"`
  `[logpath]` and `\logfile` represent the path and name of the output log file.

5 In the **Welcome** page, click **Next**.

6 In the **Symantec Endpoint Encryption Multi-Factor Authentication** page, click **Next**.

7 In the **License agreement** page, select **I accept the terms in the license agreement** and click **Next**.

8 On the **Setup Type** page, to install Management Agent, select **Custom**.

9 On the **Custom Setup** page, do the following:

- Deselect **Management Server**
- Select **Management Agent**. Choose the features that you want to enable in Management Console including:
  - Drive Encryption
  - Removable Media Encryption

Note: When you select Management Agent, the SEE Help Desk, Symantec Endpoint Encryption for BitLocker, and Symantec Endpoint Encryption for FileVault features are installed by default.

- Configure the following options for each feature:

Feature navigation tree	Lets you control how the features are installed. Click the icon that is next to the feature that you want to change and then select from the following: ■ This feature will be installed on the local hard drive ■ This feature, and all sub-features, will be installed on the local hard drive ■ This feature will not be available
Disk Usage	Lets you view the disk space that is required for the features. Select the feature that you want to view and then click **Disk Usage**.

10 In the **Token Authentication** page, you can indicate the type of token that client computers use to authenticate with Symantec Endpoint Encryption. The option that you select here affects the settings in your client installation packages.

If you do not plan to use tokens to authenticate, click **Next**.

If you do plan to use token authentication, select the type of token that you plan to use and then click **Next**.

11 In the **Database Server** page, click **Use SEE Server** to install the Management Console with the default settings.

12 In the **Database Server** field, choose the Microsoft SQL Server instance that hosts the Symantec Endpoint Encryption database. To select from a list of instances click **Browse**, or enter the NetBIOS name of the instance.

13 In the **Database Name** field, do one of the following:

- Accept the default name `SEEMSDb` if you created your database with the default name.
- If you created your database with a custom name, enter the unique custom name.

14 Click **Enable TLS/SSL** if you configured your database to use TLS/SSL encryption.

See "About configuring TLS/SSL communications for Symantec Endpoint Encryption" on page 20.

15 If you configured the database server use a custom port, click **Custom port** and then enter the custom port number. If you do not use a custom port do not click **Custom port**.

16 In the **Authentication** section, you must enter the credentials of the Policy Administrator account. Symantec Endpoint Encryption uses this account to authenticate with the Symantec Endpoint Encryption database.

Do one of the following:

- To use the credentials of the currently logged on Microsoft Windows user, click **Windows Authentication**.
- To enter the credentials of a SQL account, click **SQL Server Authentication** and enter the SQL credentials of the Policy Administrator account.

See "Accounts required by Symantec Endpoint Encryption" on page 9.

17 Click **Next**.

The installation wizard authenticates to the database server that you specified, and it verifies that the account credentials are correct.

18 In the **SEE Management Password** page, you must enter the credentials of the Management Password. The Management Password is set when you first install the Symantec Endpoint Encryption Management Server.

See "About the Management Password" on page 16.

19 Click **Next**.

20 In the **Ready to Install the Program** page, click **Install**.

21 In the **Install Wizard Completed** page, click **Finish**.

Adding or removing the Symantec Endpoint Encryption snap-ins

You can add or remove the Symantec Endpoint Encryption snap-ins that are installed using the `SEE Server Suite` file.

Therefore, you can perform the following operations, such as:

- Add Management Console and Drive Encryption and Removable Media Encryption snap-ins, if earlier only the Management Server was installed.
- Remove all the Symantec Endpoint Encryption feature snap-ins, if all the Symantec Endpoint Encryption features are installed earlier.

To add or remove the Symantec Endpoint Encryption feature snap-ins, do one of the following:

1. Double-click the `SEE Server Suite` file to run it, or
2. Use the **Add/Remove Programs** utility in the **Control Panel**.

Upgrading the Autologon Utility (optional)

The Autologon Utility lets policy administrators remotely deploy software to client computers. You can use this feature if you use preboot authentication. Because software installations typically require several restarts, the Autologon Utility lets you bypass preboot authentication.

To upgrade the Autologon snap-in:

1. On the Management Console computer, do one of the following:
   - If the computer's operating system is 32-bit, run the `SEE Autologon.MSI` file.
   - If the computer's operating system is 64-bit, run the `SEE Autologon x64.MSI` file.
2. In the **Welcome** page, click **Next**.
3. In the **License agreement** page, click **I accept the terms in the license agreement** and click **Next**.
4. In the **destination folder** page, you can change the destination of where the wizard installs the program files.

   To choose a different location to install the program files, click **Change**, or click **Next** to accept the default installation location.
5. In the **Ready to Install the Program** page, click **Install**.
6. In the **Completed** page, click **Finish**.

Note: After you upgrade your client computers, if you want to use the Autologon Utility, enable the Autologon policy option. To allow a client administrator to manage the Autologon Utility using the Administrator Command Line, ensure that you configure the **Autologon only when activated by admin locally** policy option.

Upgrading the Windows Password Reset snap-in (optional)

The Symantec Endpoint Encryption Windows Password Reset snap-in lets you assist users who have forgotten their Microsoft Windows password. You use the Symantec Endpoint Encryption Windows Password Reset snap-in to create the Windows Password Reset Utility client installer. The Windows Password Reset Utility is installed on Drive Encryption client computers and enables users to reset their Windows password when they use Drive Encryption Self-Recovery.

You run the `SEE Windows Password Reset.MSI` file to install the Symantec Endpoint Encryption Windows Password Reset snap-in into the Management Console.

To upgrade the Symantec Endpoint Encryption Windows Password Reset snap-in:

1. On the Management Console computer, do one of the following:
   - If the computer's operating system is 32-bit, run the `SEE Windows Password Reset.MSI` file.
   - If the computer's operating system is 64-bit, run the `SEE Windows Password Reset x64.MSI` file.
2. On the **Welcome** page, click **Next**.
3. On the **License agreement** page, click **I accept the terms in the license agreement** and click **Next**.
4. On the **destination folder** page, you can change the destination of where the wizard installs the Symantec Endpoint Encryption Windows Password Reset snap-in files.

   Click **Change** to choose a different location, or click **Next** to accept the default installation location.
5. On the **Ready to Install the Program** page, click **Install**.
6. On the **Completed** page, click **Finish**.

Completing the upgrade

After you finish the wizards, verify that you have set up the server and database correctly. Then, schedule regularly occurring backups of the database.

Do the following:

- Verify your server installation:
- Verify your database installation
- Back up your database

Verify your server installation:

To verify your server installation:

1. Open the Internet Information Service (IIS) Manager snap-in.
2. Expand the node for the Symantec Endpoint Encryption Management Server computer.
3. Expand **Sites**, then right-click **Symantec Endpoint Encryption Services** and click **Switch to Content View**.
4. Click **Symantec Endpoint Encryption Services**.
5. Verify that the snap-in lists the **Symantec Endpoint Encryption Services** website and that the service status is started. If the website's status is stopped, it indicates that the port number that you specified for communications with the client computers is already in use.

   Verify that the right pane contains the following items:

   - The **bin** subfolder
   - The `GECommunicationWS.asmx` file
   - The `web.config` file
6. Open the Event Viewer snap-in and examine the Application event log. Verify that there are no errors generated by the event sources **ADSyncService**.

   If you ran the MSI from the command line and enabled logging, you have logged each step of the installation process. The command line stores the log file at the path that you specified. If you did not specify a path, the files are stored in the working directory that was current when you issued the command.

Verify your database installation

To verify your database installation:

1. Access the Symantec Endpoint Encryption database with the Microsoft SQL Server Management Studio.
2. Use administrator-level privileges to verify the following:
   - The installer created a new database by the name that you specified or the default name of **SEEMSDb**.
   - The installer added the Symantec Endpoint Encryption Management Server account that you specified as a user of the new database.
   - The installer populated the new database with Symantec Endpoint Encryption–specific tables. For example, `dbo.GEMSEventLog`.
   - Open the Windows Event Viewer on the computer that hosts the Symantec Endpoint Encryption database. The viewer logs the events that are related to the creation of the

Symantec Endpoint Encryption database in the **Application** category with the source **MSSQLSERVER**. Make sure that it displays no error messages.

Back up your database

After you install and verify the Symantec Endpoint Encryption Management Server, Symantec recommends that you run a complete backup of the Symantec Endpoint Encryption database.

Symantec also recommends that you schedule regular backups of the Symantec Endpoint Encryption database.

Chapter 3

Creating installers for the Symantec Endpoint Encryption clients

This chapter includes the following topics:

About client installers

Purpose

The Symantec Endpoint Encryption client installation packages deliver the client software and initial settings to the client computers. For the Microsoft Windows client computers, the installation package contains Management Agent, either Drive Encryption or Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption. For the Macintosh client computers, the installation package contains Symantec Endpoint Encryption for FileVault.

Note: The Symantec Endpoint Encryption Client installation package also installs the Symantec Endpoint Encryption Client Administrator Console.

You create the Symantec Endpoint Encryption client installation packages from the Management Console.

Client installer package contents

The client installation packages consist of the following installers, and log files for Management Agent and the Drive Encryption or Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption features. Each log file documents the feature-specific contents of the installer and includes the file name and the date and time that the installer was created.

- BitLockerSettings month_day_year-hour.minute.sec.log
- DriveEncryptionSettings month_day_year-hour.minute.sec.log
- ManagementAgentSettings month_day_year-hour.minute.sec.log
- RemovableMediaEncryptionSettings month_day_year-hour.minute.sec.log
- SEE Client.msi
- SEE Client_x64.msi
- SEEInstaller.zip

Note: The SEEInstaller.zip folder is created to install Symantec Endpoint Encryption for FileVault on the Macintosh computers. The compressed folder consists of the SEEInstaller-<version number of the release>.<build number>.pkg and MacSettings.xml files.

Note: Dual management console functionality requires at least Symantec Endpoint Encryption 8.2.1 MP14: If you use Symantec Endpoint Encryption 11.2.0 with dual management consoles, your 8.2.1 environment requires at least Symantec Endpoint Encryption 8.2.1 MP14 if you want to generate MSIs for SEE Full Disk or SEE Removable Storage clients.

About the installation settings wizards

You can create the Symantec Endpoint Encryption Client installation package by running the Windows Client installation settings wizard from the Management Console. The wizard enables you to define policy settings for the following features:

- Management Agent

- Drive Encryption
- Symantec Endpoint Encryption for BitLocker
- Removable Media Encryption

You can create the Symantec Endpoint Encryption for FileVault installation package by running the Symantec Endpoint Encryption for FileVault installation settings wizard from the Management Console.

Note: The Symantec Endpoint Encryption for FileVault installation package does not change any policy settings. The client installation package identifies the client computers to the Symantec Endpoint Encryption Management Server for tracking and reporting purposes and for computer access recovery. Policy settings are defined using a GPO only.

On the final page of each wizard, you are prompted for a location to save the client installation settings MSI package.

For Symantec Endpoint Encryption Client, two MSI packages are saved, for 32- and 64-bit Windows editions. The 64-bit package is appended with _x64.

For Symantec Endpoint Encryption for FileVault, shown in the Management Console user interface as **Mac FileVault Client**, the MSI package is saved as a .zip folder. The SEEInstaller.zip folder consists of the SEEInstaller-<version number of the release>.<build number>.pkg and MacSettings.xml files.

Save the package in a shared network location, such as the SYSVOL folder on the domain controller.

You cannot load a previously created client installation package to examine the settings. You can know the contents of each MSI, however, in two ways:

- Save each client installer package with a descriptive name. A descriptive name is helpful if you plan to deploy multiple sets of packages throughout your organization.
- View the log files that Symantec Endpoint Encryption creates with each MSI.
  The individual settings that you selected for a given feature are saved in a date- and time-stamped log file. An example of a log file name is “ManagementAgentSettings 3_27_2014-18.21.59.log.”
  - The log file is created in the same location that you specified when you saved the package.
  - The log file does not show the contents of password fields. You should separately record and store in a secure location all passwords that you specify in an installation package.

Creating a Symantec Endpoint Encryption Client installation package

The Windows Client Installation Settings wizard walks you through a series of panels, where you choose the features that you want to include in the Symantec Endpoint Encryption Client installation package. Then, you configure the initial policy settings that are applied when Symantec Endpoint Encryption Client is installed.

See "About enabling features in the Symantec Endpoint Encryption Client installation package" on page 66.

Note: The Symantec Endpoint Encryption Client installation package always installs Management Agent. If you choose to include the Drive Encryption feature in the Symantec Endpoint Encryption Client installation package, the package also installs the Symantec Endpoint Encryption Client Administrator Console and the Administrator Command Line without any additional policy configuration.

Perform the following procedure to create an Symantec Endpoint Encryption Client installation package.

To create an Symantec Endpoint Encryption Client installation package

1. In the left pane, click **Symantec Endpoint Encryption Software Setup > Windows Client**.
2. On the **Windows Client Installation Settings – Features** page, select the features that you want to enable in the Symantec Endpoint Encryption Client installation package. Some features might not be available for selection depending upon whether they were disabled during the Symantec Endpoint Encryption Management Server installation.

   Note: For the **Disk encryption** option, you can select either the Drive Encryption feature, or Symantec Endpoint Encryption for BitLocker. If you select Drive Encryption, ensure that the Microsoft BitLocker feature is disabled on the Microsoft Windows computers on which you want to install Symantec Endpoint Encryption Client. If you select Symantec Endpoint Encryption for BitLocker, ensure that you install Symantec Endpoint Encryption Client on Windows computers that support the BitLocker feature.
3. Click **Next**.
4. On the **Windows Client Installation Settings –Management Agent** page, click **Next**.
5. Perform the procedure to configure the Management Agent installation settings in Configuring the Management Agent installation settings.

6 (Optional) If you chose to enable Drive Encryption, on the **Windows Client Installation Settings –Drive Encryption** page, click **Next**. Then, perform the procedure to configure the Drive Encryption installation settings in Configuring the Drive Encryption installation settings.

Alternatively, if you chose to enable Symantec Endpoint Encryption for BitLocker instead of Drive Encryption, on the **Windows Client Installation Settings – BitLocker** page, click **Next**. Then, perform the procedure to configure the Symantec Endpoint Encryption for BitLocker installation settings in Configuring the Symantec Endpoint Encryption for BitLocker installation settings.

7 (Optional) If you chose to enable Removable Media Encryption, on the **Windows Client Installation Settings –Removable Media Encryption** page, click **Next**.

Then, perform the procedure to configure the Removable Media Encryption installation settings in Configuring the Removable Media Encryption installation settings.

8 Click **Finish**.

9 In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.

10 (Optional) Change the default package name to a name of your choice.

11 Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

Configuring the Management Agent installation settings

After you select the Symantec Endpoint Encryption features that you want to enable, the Windows Client installation settings wizard walks you through a series of panels, where you choose your Management Agent settings. This section contains the basic steps and information to configure the Management Agent installation settings in the Windows Client installation package. To learn more about any of the options, click the link at the end of each procedure.

To configure the Management Agent installation settings

Management Agent Installation Settings – Password Authentication page

1 On the **Windows Client Installation Settings – Management Agent** page, click **Next**.

2 On the **Management Agent Installation Settings – Password Authentication** page, do the following:

- In the Simple Authentication section:
  - Select the **Enable simple authentication** option to let users authenticate at the preboot login screen using only a password.

Note: If more than one user is registered on a client computer, simple authentication is not used; the detailed login screen appears, which requires a user name and domain as well.

Note: If a user with simple authentication enabled forgets their password and invokes Drive Encryption Self-Recovery, they are prompted for their user name. This ensures that the self-recovery questions belong to that user.

- In the Password Attempts section:
  - The **Limit password attempts** option is selected by default.
    This option configures a logon delay to protect against Dictionary attack tools. When the option is selected, it enables **After <x> incorrect attempts** and **pause for <x> minutes between further attempts**. You can change the number of incorrect attempts and the pause duration. After the maximum number of consecutive incorrect attempts is reached, there is a delay of one minute, by default. You can change the default value for Drive Encryption. The delay time is 20 seconds for Removable Media Encryption and you cannot change this default value.
- In the Password Complexity section:
  - In the **Minimum password length** box, type the number of characters users' Removable Media Encryption file encryption passwords must contain. The default value is 8.
  - Provide values for the options available under the **Password must contain at least** box to bring more complexity to the user password. The options are **Non-alphanumeric characters, UPPERCASE letters, lowercase letters,** and **digits**.
  - Add any non-alphanumeric characters that you want to allow in the password in the **Non-alphanumeric characters allowed in password** box. At any time, you can click **Restore Default** to remove the characters you have added manually.

  The Password Complexity settings are enforced only for Removable Media Encryption file encryption passwords.
- In the Maximum Password Age section:
  - If you do not want Removable Media Encryption file encryption passwords to expire, select **Password never expires**.
  - To set an expiration date on Removable Media Encryption file encryption passwords:
    - Select **Password expires every <x> days**. In the **Password expires every <x> days** box, type the number of days after which users' passwords expire.

- In the **Warn users <x> before their passwords expire** box, type the number of days in advance users are prompted to change their expiring passwords.

The Maximum Password Age settings are enforced only for Removable Media Encryption file encryption passwords.

- In the Password History section:
  - To allow users to use any previously used Removable Media Encryption file encryption passwords, leave the default selection of **Any previous password can be used**.
  - To define a password history restriction, select **The last <x> passwords cannot be reused**. In **The last <x> passwords cannot be reused** box, type the number of different passwords that users must use before reverting to old passwords.

The Password History settings are enforced only for Removable Media Encryption file encryption passwords.

3 Click **Next**.

Management Agent Installation Settings – Communication page

1 On the **Management Agent Installation Settings – Communication** page, do the following:

- In the **Send status updates every <x> minutes** box, specify how frequently the client should send status updates to Symantec Endpoint Encryption Management Server. The communication interval is set to 60 minutes by default.
- Verify the **Connection Name, Server, Name, Domain,** and type the password in the **Password** box under the **Communication information** section.

2 Click **Next** and then do one of the following:

- Configure the Drive Encryption installation settings.
  See "Configuring the Drive Encryption installation settings" on page 52.
- On the **Windows Client Installation Settings – BitLocker** page, click **Next**.
- Configure the Removable Media Encryption installation settings.
  See "Configuring the Removable Media Encryption installation settings" on page 60.

Alternatively, if you chose to enable only Symantec Endpoint Encryption for BitLocker, on the **Windows Client Installation Settings – BitLocker** page,click **Finish**, and then do the following:

- In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.
- (Optional) Change the default package name to a name of your choice.

Note: If you use a custom folder location, make sure that you install the Windows Password Reset Utility at the same location as Drive Encryption is installed.

- Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

Configuring the Drive Encryption installation settings

The Windows Client installation settings wizard walks you through a series of panels, where you choose your installation settings for the features that you chose to enable. This section contains the basic steps and information to configure the Drive Encryption installation settings in the Symantec Endpoint Encryption Client installation package. To learn more about any of the options, click the link at the end of each procedure.

Note: By default, the Symantec Endpoint Encryption Client installation package also installs the Symantec Endpoint Encryption Client Administrator Console and the Drive Encryption Administrator Command Line. No additional configuration is required to enable these features.

To configure the Drive Encryption installation settings

Drive Encryption Installation Settings – Client Administrators page

1. On the **Windows Client Installation Settings – Drive Encryption** page, click **Next**.
2. On the **Drive Encryption Installation Settings – Client Administrators** page, do one of the following
   - Click **Add** to add a client administrator. Type the client administrator details in the **Account Name, Password,** and **Confirm Password** boxes.
     Check the administrative privileges that you want to assign to the client administrator. By default, the **Default admin** is checked that includes all of the available administrative privileges. To provide limited administrative privileges, uncheck **Default admin** and check one or more privileges that you want to assign from **Admin Privileges**. Click **OK** to save the newly added client administrator.
     You need to add a minimum of one client administrator to proceed to the next page of the Windows Client installation settings wizard.
   - Select an existing client administrator, and click **Edit** to edit an existing client administrator.
   - Select an existing client administrator, and click **Delete** to delete an existing client administrator. You must have at least one client administrator in the list to proceed to the next page.

- The **Action List** makes available the options to **Load client administrators from installation**, **Import client administrators from csv**, and **Export client administrators to csv**. Click the link at the end of this procedure to see the Client Administrators policy options details for how to use these actions.

3 Click **Next**.

Drive Encryption Installation Settings – Registered Users page

1 On the **Drive Encryption Installation Settings - Registered Users** page, under **Authentication Method**, select an option from the **Require registered users to authenticate with** box to configure authentication method for Drive Encryption users.

- (Default) To have users authenticate with a password, click **a password**.
- To have users authenticate with a token, click **a token**.
- To have users authenticate using either a password or a token, click **password or token**.

2 Under **User Registration**, select a user registration option to configure the user registration method for Drive Encryption users.

- (Default) To allow users to authenticate and register using a Windows user name and a Windows password or token, click **Using Windows user authentication credentials**.

  Note: The single sign-on policy is applicable only to this type of users.

- To allow users to authenticate and register using a Windows user name and a Drive Encryption password, click **Using Windows user name, non-Windows password**.

  Note: This option is not available if you have selected either **a token**, or **password or token**, from the Require registered users to authenticate with list box.

- To allow users to authenticate and register using a Drive Encryption user name and a Drive Encryption password, click **Using non-Windows username, non-Windows password**.

  Note: This option is not available if you have selected either **a token**, or **password or token**, from the Require registered users to authenticate with list box.

3 Click **Next**.

Drive Encryption Installation Settings – Single Sign-On page

1. On the **Drive Encryption Installation Settings - Single Sign-On** page, the **Enable Single Sign-On** option is checked by default. The selection of this option enables you to allow users to authenticate at preboot and directly access the client computer without authenticating at the Windows logon screen.
2. Click **Next**.

Drive Encryption Installation Settings – Self-Recovery page

1. On the **Drive Encryption Installation Settings - Self-Recovery** page, the **Enable Self-Recovery** option is checked by default. The selection of this option enables you to provide values for the **Minimum answer length, Predefined questions,** and **Number of user-defined questions required** boxes.
2. Click **Next**.

If you update this policy and your users no longer comply, the user is prompted to reconfigure their self-recovery question and answers. The prompt follows the following conditions:

- If the user has configured two questions and the policy is changed so that two questions come from the server, then the user is prompted to reconfigure their Drive Encryption self-recovery questions.
- If the user has configured two questions, and the policy is changed so that three questions are necessary, then the user is prompted to reconfigure their Drive Encryption self-recovery questions.
- If the user has configured three questions and now the policy has changed so that two questions are necessary, then the user is not prompted.

Drive Encryption Installation Settings – Startup page

1. In the **Preboot Splash Screen** section of the **Drive Encryption Installation Settings - Startup** page, do the following:
   - Click **A custom image** or **The SEE logo** to select the image that a user should see in the Drive Encryption startup screen. Alternatively, click **No splash screen** if you do not want a startup screen to precede the preboot authentication screen.
   - (Optional) If you selected **A custom image**, select either **BIOS** or **UEFI** depending on the mode in which the client computers boot. Select both of the modes if you plan to create a common installer. Click **Browse** to locate the path of the custom image that you want to set for the Drive Encryption startup screen.
     - If you selected **BIOS**, in the **Text Color** menu, set the color of the legal notice text that appears on the startup screen to either **Black** (default) or **White**. For the BIOS mode, the custom image must be in the .xpm file format.

- If you selected **UEFI**, in the **Text Color** menu, set the color of the legal notice text that appears on the startup screen to either **White** (default) or **Black**. For the UEFI mode, the custom image must be in the .bmp file format.

You can skip this step if you do not want to display a custom startup screen or a legal notice.

- Enter the **Legal Notice** text that you want to display on the startup screen. By default, the **Legal notice** box contains a standard notice from Symantec.
- Type the startup logon message in the **Logon Message** box that you want to display to registered users as they authenticate to Drive Encryption.
  The maximum number of characters displayed in the login screen is 80. In the Japanese version, the maximum is 40 because the double-byte characters occupy double the width of Latin characters.

Note: The maximum number of characters displayed in the preboot startup screen is 1024. There is also a limit of 19 lines of text; therefore, not all 1024 characters may be displayed as some longer words can cause lines to wrap early.

In the Chinese, Japanese, and Korean versions, the maximum number of characters displayed in the preboot splash screen is 512, instead of 1024. This is due to the double-byte characters occupying double the width of Latin characters when displayed.

---

2 In the **Preboot Login Screen** section, do the following:

- Click **A custom image** or **The SEE logo** to select the image that a user should see in all the Drive Encryption preboot screens.
- (Optional) If you selected **A custom image**, select either **BIOS** or **UEFI** depending on the mode in which the client computers boot. Click **Browse** to locate the path of the custom image that you want to set for the Drive Encryption preboot login screen.
  - If you selected **BIOS**, in the **Text Color** menu, set the color of the logon message that appears on the preboot login screen to either **Black** (default) or **White**. For the BIOS mode, the custom image must be in the .xpm file format.
  - If you selected **UEFI**, in the **Background Color** menu, set the background color of the logo that appears on the preboot login screen by entering values in the **Red**, **Green**, and **Blue** text boxes. These values range from 0 to 255. The default background color is yellow with the RGB value 255, 206, 0. For the UEFI mode, the custom image must be in the .bmp file format.

3 In the **Logon Customization** section, type the logon message that you want to display at Drive Encryption login screen in the **Logon Message** box.

Note: The maximum number of characters displayed in the login screen is 80. In the Chinese, Japanese, and Korean versions, the maximum number of characters displayed in the login splash screen is 40, instead of 80. This is due to the double-byte characters occupying double the width of Latin characters when displayed.

---

4 Click **Next**.

Drive Encryption Installation Settings – Logon History page

1 On the **Drive Encryption Installation Settings - Logon History** page, do the following:

- Check or uncheck **User name**.
- After you check this option, **Domain** disables, and prefills the Symantec Endpoint Encryption logon screen with the name and domain of the most recently logged on user.

2 Click **Next**.

Drive Encryption Installation Settings – Encryption page

1 On the **Drive Encryption Installation Settings - Encryption** page, do the following:

- Click **128-bit** or **256-bit** to specify the AES encryption strength in the **AES encryption strength** box. **256-bit** is selected by default.
- Select **Encrypt boot disk only** or **Encrypt all disks** to specify which disks you want to encrypt.
- Check or uncheck **Include unused disk space when encrypting disks and partitions**. This check box is selected by default. After the selection of this option, Drive Encryption includes the encryption of the unused disk space when you encrypt the disks and partitions.

  Note: Client administrators can use the Administrator Command Line to issue an `encrypt` command with a `--skip-unused-space` option, independent of this policy setting.

- Check or uncheck **Double-write sectors during encryption or decryption (May significantly increase encryption and decryption time)**. After you check this option,

every data sector is double-written during fixed disk encryption or decryption and may significantly increase encryption and decryption time.

2 Click **Next**.

Drive Encryption Installation Settings – Client Monitor page

1 On the **Drive Encryption Installation Settings - Client Monitor** page, do one of the following:

- The **Do not enforce a minimum contact period with the SEE Management Server** option is selected by default. After the selection of this option, you cannot enforce a regular network contact.
- Click **Lock computer after <x> days without contact** to force a computer lockout after a specified number of days without network contact. If you select this option, you can specify the number of days a computer may remain without network contact, from 1–365. Type the number of days in advance, from 0–364 that users are warned to connect to the network and avoid a lockout in the **Warn users <x> days before locking computer** box.

2 Click **Next**.

Drive Encryption Installation Settings – Help Desk Recovery page

1 On the **Drive Encryption Installation Settings - Help Desk Recovery** page, do the following:

- The **Enable Help Desk Recovery** option is selected by default. The selection of this option enables you to make this pre-Windows authentication assistance method available to Drive Encryption users.
- Check or uncheck **Help Desk Recovery Communication Unlock**. After you check this option, it enables the users who have been locked out of their computers for a failure to communicate to regain access using the Help Desk Recovery Program.

2 Click **Next**.

Drive Encryption Installation Settings – Self-Encrypting Drives page

1 On the **Drive Encryption Installation Settings - Self-Encrypting Drives** page, the **Use hardware encryption for compatible Opal-compliant drives** option is checked by default. The selection of this option allows hardware encryption on Opal v2 compliant drives using an Opal drive's built-in encryption capability.

For a detailed description of qualifying conditions that Opal v2 compliant drives must meet, see: http://www.symantec.com/docs/TECH226779.

Note: Drive Encryption software uses registry entries to identify which drives are whitelisted. When Symantec releases a new version of Endpoint Encryption, Symantec updates the whitelist and populates the registry entries as part of the release. If Symantec tests and approves Opal drives between releases, Symantec updates the whitelist but you must populate the new registry entries. You only need to do this if you are interested in using one or more of those drives. To see the process for creating registry entries that identify an Opal drive as whitelisted, see: http://www.symantec.com/docs/TECH235480.

---

2 If you chose to enable Removable Media Encryption, click **Next** to configure the Removable Media Encryption installation settings.

See "Configuring the Removable Media Encryption installation settings" on page 60.

Alternatively, if you chose not to enable Removable Media Encryption, click **Finish**, and then do the following:

- In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.
- (Optional) Change the default package name to a name of your choice.
- Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

Configuring the Symantec Endpoint Encryption for BitLocker installation settings

The Windows Client installation settings wizard walks you through a series of panels, where you choose your installation settings for the features that you chose to enable. This section contains the basic steps and information to configure the Symantec Endpoint Encryption for BitLocker installation settings in the Symantec Endpoint Encryption Client installation package. To learn more about any of the options, click the link at the end of each procedure.

To configure the Symantec Endpoint Encryption for BitLocker installation settings

BitLocker Installation Settings – Encryption and Authentication page

1. On the **Windows Client Installation Settings - BitLocker** page, click **Next**.
2. On the **BitLocker Installation Settings - Encryption and Authentication** page, select an encryption or a decryption policy option.
3. For the encryption policy option, do the following to select the encryption and the authentication policies:
   - To encrypt all volumes on a client computer, select **Encrypt all volumes**. This option is checked by default.
   - In the **Encryption Method** section, you must select an encryption strength; you may select an encryption mode. For all Windows systems, select 128-bit or 256-bit in the **AES encryption strength** box to specify the AES encryption strength. For systems running Windows 10 version 1511 and later, optionally also select **Prefer the XTS-AES encryption mode, if available**. The AES encryption strength that you selected is applied.

     Note: If you are installing the BitLocker client on a system with Windows 10 version 1511 earlier installed with the **Prefer the XTS-AES encryption mode, if available** option selected, then the volumes are encrypted using the AES encryption mode only.

   - In the **Authentication Method** section, select an option to specify how users gain access to the client computer. Do one of the following:
     - To have users authenticate with TPM, click **Trusted Platform Module (TPM)**. User intervention or credentials are not required to gain access to the client computer.
     - To have users authenticate with TPM and a PIN, click **TPM and PIN**. This option is selected by default. The PIN length must be 6 - 20 digits.
     - To use the password authentication method for the client computers that do not have TPM chip, or do not have TPM in a ready-to-use state, click **Fall back to password if TPM is unavailable**. This option is selected by default. The password length must be 8 - 99 characters. This policy option is supported on computers having operating system Windows 8 or later installed.
4. For the decryption policy option, select **Decrypt all volumes** to decrypt all the volumes on a client computer. Symantec Endpoint Encryption for BitLocker first decrypts all of the data volumes and then decrypts the boot volume.
5. Click **Next**.

BitLocker Installation Settings - Client Monitor page

1 On the **BitLocker Installation Settings - Client Monitor** page, choose one of the two options that you want to apply on a computer with Symantec Endpoint Encryption for BitLocker installed:

- The **Do not enforce a minimum contact period with the SEE Management Server** option is selected by default. After the selection of this option, you cannot enforce a regular network contact.
- Click **Lock computer after <x> days without contact** to force a computer lockout after a specified number of days without network contact. If you select this option, you can specify the number of days a computer may remain without network contact, from 1 - 365. Type the number of days in advance, from 0 - 364 that users are warned to connect to the network and avoid a lockout in the **Warn users <x> days before locking computer** box.

2 If you chose to enable Removable Media Encryption, click **Next** to configure the Removable Media Encryption installation settings. See "Configuring the Removable Media Encryption installation settings" on page 60.

Alternatively, if you chose not to enable Removable Media Encryption, click **Finish**, and then do the following:

- In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.
- (Optional) Change the default package name to a name of your choice.
- Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

Configuring the Removable Media Encryption installation settings

The Windows Client installation settings wizard walks you through a series of panels, where you choose your installation settings for the features that you chose to enable. This section contains the basic steps and information to configure the Removable Media Encryption installation settings in the Symantec Endpoint Encryption Client installation package. To learn more about any of the options, click the link at the end of each procedure.

About the Symantec Removable Media Encryption Burner Application

When Removable Media Encryption is installed on a client computer, the Symantec Removable Media Encryption Burner Application is also installed. The application requires the enablement of the Access and Encryption policy option 'Allow read and write access to files on removable media.'

The Symantec Removable Media Encryption Burner Application lets users encrypt and then burn files and folders onto CDs, DVDs, and Blu-ray Discs. From the client computer, a user can access the application in two ways:

- From the Windows **Start** menu, select **Symantec Removable Media Burner Application**. When the application launches, the user can access the online Help for instruction on using the interface.
- From the command line, run the Removable Media Encryption Burner Application command line. For more information, see the *Symantec Endpoint Encryption 11.2.0 Removable Media Encryption Burner Application Command line Guide*.

To configure the Removable Media Encryption installation settings

Removable Media Encryption Installation Settings - Access and Encryption page

1. On the **Windows Client Installation Settings – Removable Media Encryption** page, click **Next**.
2. On the **Removable Media Encryption Installation Settings - Access and Encryption** page, do the following:
   - In the **Access** section, do one of the following:
     - Click **Do not allow access to files on removable media** to deny read and write access to the files and folders that are stored on removable media, even if a user is registered to Symantec Endpoint Encryption.
     - Click **Allow read-only access to files on removable media** to allow the users to read the files that are stored on removable media. If the files are encrypted, users must provide the credentials that are used to encrypt the file to read its contents. In such a case, the users cannot write files to removable media.
     - Click **Allow read and write access to files on removable media** option to allow the users to read and write files to removable media. If the files are encrypted, users must provide the credentials that are used to encrypt the file to read its contents. This option is selected by default.
       When you select this option, the options for **Encryption Format**, **Automatic Encryption**, and **On-Demand Encryption** are available.
   - In the **Encryption Format** section, do one of the following:
     - Click **SEE RME** to encrypt files to removable media using the Symantec Endpoint Encryption Removable Media Encryption 11.x format. This option is selected by default.
     - Click **SEE RS** to encrypt files to removable media using the Symantec Endpoint Encryption Removable Storage 8.2.1 format.

Select this option if your users move files between the computers that are running 11.x and 8.2.1 software. This encryption format is backward-compatible and computers running either version of the software can read these files.

- In the **Automatic Encryption** section, do one of the following:
  - Click **Do not encrypt** not to encrypt files on removable media.
  - Click **Encrypt files as per Symantec Data Loss Prevention** to use the detection and the response capabilities of Symantec Data Loss Prevention to dictate the encryption of files.
  - Click **Encrypt new files** to automatically encrypt all files newly added to removable media. This option is selected by default.

    Note: To exclude multimedia files or certain file types from automatic encryption, you can select more options on the **Device and File Type Exclusions** page.

  - Click **Allow users to choose** if you want to let the users choose whether or not to automatically encrypt new files. Under the **Allow users to choose** option, select the default behavior that you want to happen if your users do not make a choice. Choose either **Default to encrypt new files**, or **Default to do not encrypt**.
- In the **On-Demand Encryption** section, you can:
  - Check **Users can right-click to encrypt existing files on removable media** to provide the users with the ability to encrypt files on removable media using a right-click menu. This option is selected by default.
  - Check **Users can right-click to decrypt existing files on removable media** to provide the users with the ability to decrypt files on removable media using a right-click menu.
    If **Encrypt files as per Symantec Data Loss Prevention** is selected, Symantec recommends unchecking both options.

3 Click **Next**.

Removable Media Encryption Installation Settings - Device and File Type Exclusions page

1 On the **Removable Media Encryption Installation Settings - Device and File Type Exclusions** page, do the following:

- In the **Exemption for Multimedia Files** section, check or uncheck **Exclude multimedia files from automatic encryption**. Even if you select the **Encrypt new files** option on the **Access and Encryption** page, you can exempt certain types of multimedia files from automatic encryption by checking **Exclude multimedia files from automatic encryption**. Then leave selected one or more of the following check boxes according to the type of multimedia file formats you want to exclude from encryption:

- **Audio**
- **Video**
- **Image**

- In the **File Types Exclusion** section,
  - Check or uncheck **Exclude file types extensions from automatic encryption (comma separated)**. Check this option, and type the file type extensions, such as .jpeg, .exe, and so on that are excluded from automatic encryption.
- In the **Device Exclusions** section, check or uncheck **Exclude these removable media encryption devices from encryption**. Do one of the following to exempt removable media encryption devices from encryption:
  - To exempt a specific device from a vendor, enter the vendor ID, product ID, and an optional description in the fields provided.
  - To exempt all the devices from a vendor, type the vendor ID in the **Vendor ID** box. Also type the wildcard character * in the **Product ID** box and an optional description in the **Description (Optional)** box.

2 Click **Next**.

Removable Media Encryption Installation Settings - Encryption Method page

1 On the **Removable Media Encryption Installation Settings - Encryption Method** page, do one of the following:

- The **A password** option is selected by default. The selection of this option enables the users to restrict the encryption method to a password.
- Click **A certificate** so that users can restrict the encryption method to one certificate.
- Click **A password and/or certificate** to let each user choose the encryption method of password, certificate, or both.

2 Click **Next**.

Removable Media Encryption Installation Settings - Default Passwords page

1 On the **Removable Media Encryption Installation Settings - Default Passwords** page, do the following:

- In the **Default Password** section, do one of the following:
  - To allow users to set a default password, click **Allow users to set a default password**. This option is chosen by default.
    - To apply password aging to default passwords, check **Apply password aging to Removable Media Encryption default passwords**. This option ensures that users set default passwords that conform to the restrictions that you define.

These restrictions are defined in the **Maximum Password Age** and **Password History** sections of the Management Agent Password Authentication policy. These settings define expiration dates and restrict password reuse.

Note: If you let users set a default password, you can also let them set session passwords. You cannot allow both default passwords and device session passwords to be set.

- To prevent users from setting a default password, click **Do not allow users to set a default password**.

- If the **Session Passwords** section is available, do one of the following:
  - To allow users to set session passwords, click **Allow users to set session passwords**; otherwise, click **Do not allow users to set session passwords**.
    If you let users set session passwords, choose the password expiration method:
    - To permanently expire (delete) session passwords at the end of each Windows session, click **Delete session passwords at the end of every Windows session**. Users must recreate the passwords.
    - To temporarily expire (deactivate) session passwords at the end of each Windows session, click **Deactivate session passwords at the end of every Windows session, but allow them to persist across every Windows session**. Passwords remain on the user's computer, but the user must toggle them on.
    - To apply password aging to session passwords, click **Apply password aging to session passwords**. This option ensures that users set session passwords that conform to the restrictions that you define. These restrictions are defined in the **Maximum Password Age** and **Password History** sections of the Management Agent Password Authentication policy. These settings define expiration dates and restrict password reuse.
    - To prevent session passwords from expiring, click **Do not delete or deactivate session passwords**. This option is chosen by default.

- If the **Device Session Password** section is available, do one of the following:
  - To allow users to set device session passwords, click **Allow users to set a device session password for each removable media encryption device**. Device session passwords are useful in a kiosk environment.

Note: If you enable device session passwords, you cannot use recovery certificates. Even if you enable certificates on the **Recovery Certificate** page, Removable Media Encryption ignores them.

- If you do not want users to set device session passwords, click **Do not allow users to set a device session default password for each removable device**. This option is chosen by default.

2 Click **Next**.

See "Configuring the Management Agent installation settings" on page 49.

Removable Media Encryption Installation Settings - Recovery Certificate page

Note: Use the Recovery Certificate policy to include the copy of the Recovery Certificate that does not have the private key in the Removable Media Encryption package. Upon receipt, clients begin to encrypt files using this Recovery Certificate in addition to the user's credentials. The Recovery Certificate policy only applies to computers on which write access and encryption are enabled for removable media devices.

1 On the **Removable Media Encryption Installation Settings - Recovery Certificate** page, do one of the following:

- Click **Do not encrypt files with a recovery certificate** not to include a copy of the Recovery Certificate in the client installation package. This option is selected by default.
- Click **Encrypt files with a recovery certificate** if you want to use a Recovery Certificate.

Note: If you enable device session passwords on the **Default Passwords** page, Removable Media Encryption ignores recovery certificates.

- You are prompted for the location of the PKCS#7 format certificate file (.p7b), choose a certificate file.
- Click **OK**.
- On the **Recovery Certificate** page, the issuer and serial number of the certificate appears. Click **Change Certificate** to select a different certificate file.

2 Click **Next**.

Removable Media Encryption Installation Settings - Portability page

1 On the **Removable Media Encryption Installation Settings - Portability** page, do the following:

- In the **Access Utility** section:
  - Check or uncheck **Copy the Removable Media Access Utility for Windows to removable media**. After you check this option, it enables you to write Removable Media Access Utility that runs on Windows computers to removable media automatically.
  - Check or uncheck **Copy the Removable Media Access Utility for Mac OS X to removable media**. After you check this option, it enables you to write Removable Media Access Utility that runs on Mac OS X computers to removable media automatically.
- In the **Self-Decrypting Archive** section:
  - Check or uncheck **Allow users to save files as password encrypted self-decrypting archive**. After you check this option, it enables you to permit users to create self-decrypting archives.

2 Click **Next**.

Removable Media Encryption Installation Settings - Expired Certificates page

1 On the **Removable Media Encryption Installation Settings - Expired Certificates** page, do one of the following:
   - Check **Users can use expired certificates to encrypt files** so that the user can encrypt the file using an expired certificate.
   - If you uncheck this option, the user cannot use an expired certificate for file encryption.
2 Click **Finish**.
3 In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.
4 (Optional) Change the default package name to a name of your choice.
5 Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

About enabling features in the Symantec Endpoint Encryption Client installation package

When you create a Symantec Endpoint Encryption Client installation package, you enable features depending upon your organization's security requirements. Use the Windows Client Installation Settings wizard to specify the features that you want to enable in Symantec Endpoint Encryption Client. The Symantec Endpoint Encryption Client installation package contains the policy settings for all of the features that you enable. This topic provides information about enabling features in the Symantec Endpoint Encryption Client installation package.

On the **Windows Client Installation Settings – Features** page of the Windows Client Installation Settings wizard, you can choose to enable the following features:

- For disk encryption:
  - Drive Encryption, or
  - Symantec Endpoint Encryption for BitLocker
- Removable Media Encryption

You cannot install both Drive Encryption and Symantec Endpoint Encryption for BitLocker on the same client computer. If you already have Drive Encryption installed, you cannot enable Symantec Endpoint Encryption for BitLocker. Similarly, if you already have Symantec Endpoint Encryption for BitLocker installed, you cannot enable Drive Encryption. However, you can enable Removable Media Encryption with either feature.

Enabling features during upgrades

The following tables provide feature selection information for upgrades, depending upon the product and version that is currently installed.

Table 3-1 Enabling features when upgrading from Symantec Endpoint Encryption 11.0.x or later

Features that are already installed	Additional 11.2.0 features that you want to install during the upgrade	Features that you must enable in the client installation package
Drive Encryption	None	Drive Encryption
Removable Media Encryption	None	Removable Media Encryption
Drive Encryption	Removable Media Encryption	■ Drive Encryption ■ Removable Media Encryption
Removable Media Encryption	Drive Encryption	■ Drive Encryption ■ Removable Media Encryption
Drive Encryption	Symantec Endpoint Encryption for BitLocker	This is not a valid feature combination.
Removable Media Encryption	Symantec Endpoint Encryption for BitLocker	■ Symantec Endpoint Encryption for BitLocker ■ Removable Media Encryption
■ Drive Encryption ■ Removable Media Encryption	None	■ Drive Encryption ■ Removable Media Encryption

Table 3-1 Enabling features when upgrading from Symantec Endpoint Encryption 11.0.x or later *(continued)*

Features that are already installed	Additional 11.2.0 features that you want to install during the upgrade	Features that you must enable in the client installation package
■ Drive Encryption ■ Removable Media Encryption	Symantec Endpoint Encryption for BitLocker	This is not a valid feature combination.

Table 3-2 Enabling features when upgrading from Symantec Endpoint Encryption 8.2.1

Features that are already installed	Additional 11.2.0 features that you want to install during the upgrade	Features that you must enable in the client installation package
Symantec Endpoint Encryption Full Disk	None	Drive Encryption
Symantec Endpoint Encryption Removable Storage	None	Removable Media Encryption
Symantec Endpoint Encryption Full Disk	Removable Media Encryption	■ Drive Encryption ■ Removable Media Encryption
Symantec Endpoint Encryption Removable Storage	Drive Encryption	■ Drive Encryption ■ Removable Media Encryption
Symantec Endpoint Encryption Full Disk	Symantec Endpoint Encryption for BitLocker	This is not a valid feature combination.
Symantec Endpoint Encryption Removable Storage	Symantec Endpoint Encryption for BitLocker	■ Symantec Endpoint Encryption for BitLocker ■ Removable Media Encryption
■ Symantec Endpoint Encryption Full Disk ■ Symantec Endpoint Encryption Removable Storage	None	■ Drive Encryption ■ Removable Media Encryption
■ Symantec Endpoint Encryption Full Disk ■ Symantec Endpoint Encryption Removable Storage	Symantec Endpoint Encryption for BitLocker	This is not a valid upgrade.

Table 3-3 Enabling features when upgrading from Symantec Encryption Desktop 10.3.2 MP4 for Windows, or later

Features that are already installed	Additional 11.2.0 features that you want to install during the upgrade	Features that you must enable in the client installation package
Symantec Encryption Desktop	None	Drive Encryption
Symantec Encryption Desktop	Removable Media Encryption	■ Drive Encryption ■ Removable Media Encryption OR Enable only Removable Media Encryption, if you do not want to upgrade to Drive Encryption.
Symantec Encryption Desktop (with the Symantec Drive Encryption feature enabled)	Symantec Endpoint Encryption for BitLocker	This is not a valid upgrade.
Symantec Encryption Desktop (with the Symantec Drive Encryption feature enabled)	■ Symantec Endpoint Encryption for BitLocker ■ Removable Media Encryption	This is not a valid upgrade.
Symantec Encryption Desktop (with the Symantec Drive Encryption feature disabled)	Symantec Endpoint Encryption for BitLocker	Symantec Endpoint Encryption for BitLocker
Symantec Encryption Desktop (with the Symantec Drive Encryption feature disabled)	■ Symantec Endpoint Encryption for BitLocker ■ Removable Media Encryption	■ Symantec Endpoint Encryption for BitLocker ■ Removable Media Encryption

Creating a Symantec Endpoint Encryption for FileVault installation package

The Mac FileVault Client installation wizard walks you through a series of panels, where you choose your policy settings. You must perform the following steps to successfully create a Symantec Endpoint Encryption for FileVault installation package from the Management Console.

To create a Symantec Endpoint Encryption for FileVault installation package

1. In the left pane, click **Symantec Endpoint Encryption Software Setup** > **Mac FileVault Client**.
2. On the **Create Mac OS X Installer - Introduction** page, click **Next**.

3 On the **Create Mac OS X Installer – Institutional Recovery Key** page, do the following:

- (Default) Select the **Use an Institutional Recovery Key** check box. The selection of this option enables you to include an Institutional Recovery Key certificate in the install-time policy.
- Click **Change Key** to locate the path of the Institutional Recovery Key certificate, and select it.
- After you select the Institutional Recovery Key certificate, the name of the provider and the serial number of the Institutional Recovery Key appear in the **Issued By** and **Serial** boxes on the **Create Mac OS X Installer – Institutional Recovery Key** panel. To select a different Institutional Recovery Key certificate file, click **Change Key**.

4 Click **Next**.

5 On the **Create Mac OS X Installer - Communication** page, do the following:

- In the **Send status updates every <x> minutes** box, specify how frequently the Symantec Endpoint Encryption for FileVault client should send status updates to Symantec Endpoint Encryption Management Server. The communication interval is set to 60 minutes by default.
- Verify the **Connection Name**, **Server**, **Name**, **Domain**, and type the password in the **Password** box under the **Communication information** section.

6 Click **Finish**.

7 In the **Save Mac Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption for FileVault installation package.

8 If required, change the default Symantec Endpoint Encryption for FileVault package name.

9 Click **Save** to create the Symantec Endpoint Encryption for FileVault installer with the administrative policies you have configured at your desired location.

Creating a Windows Password Reset Utility installation package

The Symantec Endpoint Encryption Windows Password Reset snap-in enables you to create a Windows Password Reset Utility installation package. When you install the Windows Password Reset Utility on a Drive Encryption client computer, the utility extends the functionality of the Drive Encryption Self-Recovery feature and the Help Desk Recovery feature to enable users to reset their Windows password by themselves. Use the Windows Password Reset Utility to reduce support calls to the local help desk when users forget their Windows password.

Note: To create a Windows Password Reset Utility installation package, you must have either the Server Administrator role or the Setup Administrator role. If the policy administrator enabled the Windows Password Reset using Drive Encryption Self-Recovery, existing registered users are automatically prompted to reconfigure their security questions and answers in Drive Encryption Self-Recovery wizard after the Windows Password Reset Utility is installed.

To create a Windows Password Reset Utility MSI file

1. In the left pane of the Management Console, click the **Symantec Endpoint Encryption Windows Password Reset** snap-in.
2. On the **Windows Password Reset - Management Password Authentication** page, in the **Management** Password field, type the management password.
3. Click **Next**.
4. On the **Windows Password Reset - Settings** page, check one or more of the following options:
   - **Drive Encryption Self-Recovery** - Enables users to reset their Windows password using the Drive Encryption Self-Recovery feature.
   - **Help Desk Recovery** - Enables users to reset their Windows password using the Help Desk Recovery feature.
5. Click **Finish** and save the MSI file at the desired location.

Note: If you use a custom folder location, make sure that you install the Windows Password Reset Utility at the same location as Drive Encryption is installed.

About the Autologon Utility

Use the Autologon Utility to configure Microsoft Windows client computers to bypass the preboot authentication screen that Symantec Endpoint Encryption Management Server enforces. By default, the Autologon function is not in effect for a computer. As an administrator, you can use Autologon when you want to update or deploy software on a client computer that requires multiple restarts. Patch management is an example of a process that can require multiple restarts.

Caution: A client computer running the Autologon utility is in a state of heightened vulnerability. Using Autologon inappropriately weakens the data protection that Drive Encryption provides. To minimize the associated risks, carefully review your procedures for enabling and disabling the Autologon function. The Autologon function should be disabled immediately when its intended use is achieved. For example, ensure that you disable the Autologon function immediately after you finish updating client computers.

To make the Autologon Utility available to client computers, generate Autologon client MSI files. You can create an MSI file in an enabled or disabled state. After you deploy and install the Autologon MSI on client computers, client administrators can use the Drive Encryption Administrator Command Line to manage Autologon. They can override the existing policy and enable or disable the Autologon functionality, as needed.

See "Creating Autologon MSI files" on page 72.

Creating Autologon MSI files

Pre-requisite: Make sure that you have installed the Autologon Utility and added it to the Management Console as a snap-in. For more information, see the "Adding the Autologon snap-in to the Management Console" topic in the *Symantec Endpoint Encryption Installation Guide*.

To create Autologon client MSI files

1. In the left pane of the Management Console, click **Symantec Endpoint Encryption Autologon Utility**.
2. On the **Autologon Utility - Settings** page, in the **Management password** field, type the management password that is currently in use.
3. Under Autologon, do one of the following:
   - To enable the Autologon feature and create the `Autologon Infinite` MSI file, click **Always Autologon**.
   - To disable the Autologon feature and create the `Autologon NoAutologon` MSI file, click **Autologon only when activated by admin locally**.
4. Under **Autologon Precedence**, do one of the following:
   - To enable users to log on to a locked out computer when Autologon is enabled, click **Autologon takes precedence over client monitor lockout**.
   - To prevent users from logging on to a locked out computer when Autologon is enabled, click **Client monitor lockout takes precedence over Autologon**.
5. To enable Trusted Platform Module (TPM) based authentication for Autologon users, under **TPM Settings**, check **Use TPM if available**

Notes:

- This section is available only as an install-time policy setting when you create a new Autologon Utility installer.
- TPM-based authentication for Autologon requires the Microsoft Windows 10 operating system running in UEFI mode on devices that have a TPM 2.0 chip installed.
- To ensure compatibility with the TPM-based authentication for AutoLogon feature on Dell Latitude 7370, E5470, and E5570 laptops and on Dell Precision 3510 laptops, make sure that their System BIOS firmware is up to date. For more information, see http://www.dell.com/support/home/us/en/04/drivers/driversdetails?driverId=K55T9.
  In addition, use the Dell TPM 2.0 Firmware Update Utility to ensure that the TPM 2.0 firmware on these devices is up to date. For more information, refer to Dell Knowledge Base article SLN305057.

6 Click **Finish** and save the MSI file.

Note: If you want to deploy, save the created MSI files in a folder that is in a shared network location. For example, the location can be in the domain controller's SYSVOL folder.

See "About the Autologon Utility" on page 71.

See "Installing an Autologon MSI file on a client computer" on page 73.

Installing an Autologon MSI file on a client computer

Caution: A client computer running Autologon is in a state of heightened vulnerability. To minimize the associated risks, carefully review your procedures for enabling and disabling Autologon. Autologon should be disabled immediately when its intended use is achieved.

Note: If you installed the Symantec Endpoint Encryption Client to a custom installation folder, make sure that you install the Autologon Utility in the same location.

To install an Autologon MSI file on a client computer

1 Navigate to the folder in which you saved the Autologon client MSI file that you created.

2 Double-click the MSI file that you want.

3 Restart the computer.

- If the MSI file is `Autologon NoAutologon`, after the restart the user is prompted to authenticate during preboot.

- If the MSI file is `Autologon Infinite`, after the restart the user is no longer prompter to authenticate during preboot

On a client computer, to enable, disable, or set the count of authentication bypasses, a client administrator can use the Drive Encryption Administrator Command Line. For more information, see the *Symantec Endpoint Encryption Drive Encryption Administrator Command Line Guide*.

See "About the Autologon Utility" on page 71.

See "Creating Autologon MSI files" on page 72.

Chapter 4

Upgrading clients to Symantec Endpoint Encryption 11.2.0

This chapter includes the following topics:

About upgrading your Microsoft Windows clients

This topic is applicable only when you upgrade your client computers.

You can upgrade your client computers to Symantec Endpoint Encryption 11.2.0. The upgrade process lets you upgrade your client computers to the latest version of encryption products without decrypting your computers. Symantec Endpoint Encryption keeps your user data encrypted and retains the relevant metadata that it requires.

Symantec Endpoint Encryption 11.2.0 supports client upgrades from the following earlier products:

- Symantec Endpoint Encryption 8.2.1
- Symantec Endpoint Encryption 11.0.x
- Symantec Encryption Desktop 10.3.2 MP4 for Windows or later

You must run the Symantec Endpoint Encryption Client installation package to complete the upgrade of the client computer. You upgrade the clients by running `msiexec` commands.

The installer first checks the drive to determine if it can successfully upgrade. If the check passes, it backs up the metadata that is necessary for data decryption. It also preserves certain data such as preboot, drivers, and volume files so that it can keep the disk's I/O functions operational during the upgrade process.

After you upgrade, when the user restarts the computer the first time, preboot authentication is bypassed and the computer boots to Microsoft Windows. After the user logs on to Microsoft Windows for the first time, the user account is automatically registered with the client. After the next restart, the user can enter these credentials for preboot authentication. If the GPO or native policy prevents automatic registration, then preboot authentication continues to be bypassed.

If the client cannot connect to the Symantec Endpoint Encryption Management Server, it uses the policy configuration that you define in the installation MSI files. Later, if the client connects to the Symantec Endpoint Encryption Management Server, it then synchronizes its policies with the server's native policies or GPO policies.

After upgrade, auto-encryption starts on the non-encrypted partition or disk according to the encryption policy that is defined in installer (Auto-Encrypt Boot Disk/All Disk). It will have the same encryption parameters (AES cipher strength, block cipher mode) that was present with the already encrypted partitions/disk before the upgrade.

Note: When you upgrade the Symantec Endpoint Encryption Client, you must also upgrade any additional features that are installed, such as the Autologon Utility and the Windows Password Reset Utility.

About the version 11.0.x upgrade scenario

As of Symantec Endpoint Encryption 11.2.0, the Symantec Endpoint Encryption Client installation package upgrades all of the client features together. You no longer have to upgrade Management Agent, Drive Encryption, and Removable Media Encryption separately.

About the version 8.2.1 in-place upgrade scenario

In an in-place upgrade scenario, you first upgrade the Symantec Endpoint Encryption Management Server to the latest version. After you upgrade the server, you use it to generate the new Symantec Endpoint Encryption 11.2.0 client installation files. You then use these files to upgrade your existing clients to the latest version.

Note: You can still use your upgraded Symantec Endpoint Encryption Management Server to manage Symantec Endpoint Encryption 8.2.1 client computers.

About the version 8.2.1 migration scenario

In a migration scenario, you use two management servers. You keep your existing Symantec Endpoint Encryption 8.2.1 Management Server and you install a new Symantec Endpoint Encryption Management Server 11.2.0 on another computer. This approach lets you manage clients separately. You can manage Symantec Endpoint Encryption 8.2.1 clients on the Symantec Endpoint Encryption 8.2.1 server. You can manage Symantec Endpoint Encryption 11.2.0 clients on Symantec Endpoint Encryption Management Server 11.2.0. Over time, you can then migrate your previous clients to report to Symantec Endpoint Encryption Management Server 11.2.0.

To migrate, you first install the new Symantec Endpoint Encryption Management Server on a new computer. You then use it to generate the new client MSI files and then deploy them on the client computer. After the client computer is upgraded it reports to the new Symantec Endpoint Encryption Management Server.

Note: Although the client computer stops reporting to the Symantec Endpoint Encryption 8.2.1 server, the server may still keep a record of the client computers. However, the clients enforce their new policy settings and report to the new Symantec Endpoint Encryption Management Server once they establish a connection to it.

About the Symantec Encryption Desktop 10.3.2 in-place upgrade scenario

In an in-place upgrade scenario, you can upgrade a Symantec Encryption Desktop client from version 10.3.2 MP4 or later to Symantec Endpoint Encryption 11.2.0 without needing to decrypt the disk.

Note: Upgrades to Symantec Endpoint Encryption might fail if the disk partition sizes were modified after the disk was encrypted using Symantec Encryption Desktop. In such scenarios, users are recommended to first decrypt and uninstall Symantec Encryption Desktop, followed by installation of Symantec Endpoint Encryption and encryption of disks.

When you upgrade and install Drive Encryption, only the encrypted data and the metadata that is required to decrypt is migrated. Other data, such as the data for registered users, self-recovery data, and administrators are not migrated. Your users must register with Symantec Endpoint Encryption after the upgrade. The upgraded computer's state is the same as a computer with a new installation of Symantec Endpoint Encryption, except that the disk is already encrypted.

Before upgrading your Microsoft Windows clients

Consider the following before upgrading your clients:

- Back up your data.
  As with any upgrade procedure involving encryption products, there is always the risk that unexpected problems can interrupt the upgrade process. Symantec recommends that you always back up your data before you attempt an upgrade.
- If you upgrade a client using a Symantec Endpoint Encryption Client installation package that was created using a different Symantec Endpoint Encryption Management Server, the Help Desk Recovery feature stops working as the client computer does not exist in the new server's database. After the upgrade is complete, ensure that the client checks in with Symantec Endpoint Encryption Management Server. Then, disable and re-enable the Help Desk Recovery feature through the policy settings.
- Saved all of your work and closed any open files.
- Closed any third-party programs that read or write to the disk or read or write to removable media.
- Dismounted and disconnected any removable media from the client computer.
- Ensured that the disk is either completely encrypted or decrypted. If encryption or decryption is in progress, wait until the disk is completely encrypted or decrypted.
- The system requirements for upgrades also include all of the standard Symantec Endpoint Encryption 11.2.0 system requirements.
- Your environment must have Symantec Endpoint Encryption Management Server 11.2.0.
- Ensure that you have installed all of the latest Windows Updates from Microsoft. Ensure that you restart your computer after the Windows Updates are completed.
- Ensure that any pending restart due to installation of earlier version of Symantec Endpoint Encryption must be completed.
- Version 1 hardware-encrypted Opal drives are not supported. If you have v1 Opal Drives, they must be software-encrypted. Opal drives remain software encrypted and are not converted to hardware encryption.
- You cannot upgrade partially-encrypted drives.
- You cannot upgrade partially-encrypted partitions.
- You cannot upgrade disks with more than ten logical partitions.
- You cannot upgrade if encryption or decryption is still in progress
- Dual Boot is not supported
- Symantec Endpoint Encryption 11.2.0 does not support upgrades from CPA releases of Symantec Encryption Desktop 10.3.2 for Windows

Special considerations before you upgrade 8.2.1 client computers

Consider the following before upgrading your 8.2.1 clients:

- Managing Symantec Endpoint Encryption 11.2.0 clients with a Symantec Endpoint Encryption 8.2.1 server is not supported.
  Managing Symantec Endpoint Encryption 8.2.1 clients with a Symantec Endpoint Encryption Management Server 11.2.0 server is supported.
- Do not deploy Symantec Endpoint Encryption 8.2.1 policies to 11.2.0 clients.
  You cannot manage 11.2.0 clients with a Symantec Endpoint Encryption 8.2.1 server. Make sure that you configure your client to only report to, and download data from the 11.2.0 server. After you upgrade a client to 11.2.0, only 11.2.0 policies can apply to it.
- The upgrade does not preserve policy settings during the upgrade. Instead, the install policy settings from the Symantec Endpoint Encryption 11.2.0 installers take effect after the upgrade. They take effect until the client can connect to Symantec Endpoint Encryption Management Server to retrieve policies.
- Randomly generated client data is refreshed
  The randomly generated Machine IDs, or Disk IDs, policies, and client administrators are removed and refreshed during the upgrade. The Machine IDs and Disk IDs may be reported twice during the upgrade process. This behavior indicates that the IDs have been modified. This behavior is expected.
- Removable Media Encryption supports the 8.2.1 RS encryption format. The upgrade preserves your users' Removable Storage settings. After you upgrade to Removable Media Encryption you can access RS-encrypted data through the same authentication methods that you used with Removable Storage
- Hidden and system partitions are now encrypted in 11.2.0. After you upgrade a client computer from the 8.2.1 version to the 11.2.0 version of Symantec Endpoint Encryption, when a user restarts the computer and logs on to Windows, almost immediately messages appear. The notifications are for the start and completion of encryption. The hard disk is not being re-encrypted. These notifications refer to the hidden and system partitions. This behavior is normal. However, the partitions are small, the process is quick, and the messages are fleeting; therefore, some users find the messages confusing. To read the messages, a user can use the Windows Event Log Viewer. They should look for messages such as, "Encryption started on boot drive by the Drive Encryption service."
- Be aware that when upgrading from legacy versions, the upgrade does not preserve authentication data. The users must re-register.
- Be aware that after the upgrade of legacy versions, smart card users must re-enroll to be able to authenticate to preboot.

Data handling for 8.2.1 client upgrades

The upgrade preserves the following data:

- The workstation encryption keys (WEK) and disk encryption keys (DEK)
- The encryption status

- The original Master Boot Record (MBR)

The Removable Media Encryption upgrade preserves the following:

- Default Password
- Session Password 1
- Session Password 2
- Default Password Memo
- Session Password 1 Memo
- Session Password 2 Memo
- The Default Certificate information
- The “user choice” feature’s settings

The upgrade changes the following:

- The Drive Encryption policy settings. These settings include Single-Sign-on (SSO), Drive Encryption Self-Recovery, and Help Desk Recovery settings
- The client administrator credentials

All other data is removed. This data includes your existing user records. After the upgrade, each user must log on to Microsoft Windows at least once to register for preboot authentication.

Special considerations when upgrading a Symantec Encryption Desktop 10.3.2 client computer

Consider the following before upgrading your 10.3.2 clients:

- When upgrading from 10.3.2, the clients must run Symantec Encryption Desktop 10.3.2 MP4, or above.
- Symantec Encryption Desktop Drive Encryption encrypted removable disks and encrypted USB drives are not upgraded.
  You must first decrypt your removable disks, and drives before you upgrade.
- You cannot upgrade to Symantec Endpoint Encryption for BitLocker while the Symantec Drive Encryption component of Symantec Encryption Desktop is enabled.
  The following 10.3.2 Symantec Encryption Desktop components are unaffected by the upgrade process. These components continue to run and report to the 3.3.2 Symantec Encryption Management Server and can run in parallel with Symantec Endpoint Encryption:
  Symantec Desktop Email Encryption
  Symantec File Share Encryption
  PGP Shredder
  PGP Viewer
  PGP ZIP

Virtual Disk

- Be aware that when upgrading from legacy versions, the upgrade does not preserve authentication data. The users must re-register.
- Be aware that after the upgrade of legacy versions, smart card users must re-enroll to be able to authenticate to preboot.

Using the re-encrypt command after upgrading 10.3.2 clients:

The eedAdminCli includes a new command that lets you re-encrypt the disk using a new session key. This command changes the block cipher mode from PlumbCFB to CBC.

The command is:

```
--re-encrypt
```

For example:

```
eedAdminCli.exe --re-encrypt --disk <disk_id> --au <client_Administrator Name>
--ap <client_Administrator passphrase>
```

Consider the following:

- The re-encrypt command only changes the block cipher mode from PlumbCFB to CBC (zero to three). It does not change the AES Strength of the disk which is already encrypted.
- Re-encryption is blocked for new 11 clients and all other clients that are upgraded from 8.2.1 or 11.0.x.
- Re-encryption works only at the time that the fully encrypted clients are upgraded. After the block cipher mode is changed, the command will not run.
- The client administrator cannot trigger decryption until after the re-encryption process finishes. However the users can pause and resume the re-encryption process.
- The status message: “**re-encryption is in progress**” status is displayed for the command line interface as well as in the user interface.
- The Symantec Endpoint Encryption Management Console does not display any information for the re-encryption process. However, an audit event is sent to the server to indicate the start and completion of the re-encryption process.

Upgrading your Microsoft Windows clients

You can use the command line to upgrade clients to specify an output log file that you can use to troubleshoot any installation problems.

Note: When upgrading **10.3.2** client computers, decrypt your removable disks and drives before you upgrade.

To upgrade the client computers:

1 Ensure that the client computer has a stable power supply. A power failure might interrupt the upgrade process and cause it to fail.

2 Back up the computer and its data before you attempt to upgrade.

3 Confirm that the client computer meets the system requirements to run the Symantec Endpoint Encryption Client software.

Note: Symantec recommends that when installation or upgrade is in progress, you should inform the users that they should not restart their computer.

---

4 Generate your client installation MSI file.

See "Creating a Symantec Endpoint Encryption Client installation package" on page 48.

5 Copy the installation .MSI file to the local hard disk of the computer on which you want to perform the upgrade.

- If the computer's operating system is 32-bit, copy the `SEE Client.msi` file.
- If the computer's operating system is 64-bit, copy the `SEE Client x64.msi` file.

Note: If you upgrade a client using a Symantec Endpoint Encryption Client installation package that was created using a different Symantec Endpoint Encryption Management Server, the Help Desk Recovery feature stops working as the client computer does not exist in the new server's database. After the upgrade is complete, ensure that the client checks in with Symantec Endpoint Encryption Management Server. Then, disable and re-enable the Help Desk Recovery feature through the policy settings.

---

6 Depending on the version of Microsoft Windows, do one of the following:

On **Windows 7**:	Click **Start > All Programs > Accessories**. Right-click **Command Prompt** and select **Run as administrator**.
On **Windows 8.x**:	From the **Start** screen, access the **Apps** menu. In the **Windows System** section, right-click **Command Prompt** and select **Run as administrator**.
On **Windows 10**:	Click **Start > All Apps**. In the **Windows System** section, right-click **Command Prompt** and select **Run as administrator**.

If you are prompted, enter the credentials of a domain administrator account.

7 In the Command Prompt window, enter the following:

```
MSIEXEC /i "[path]\msifile" /l*v "[logpath]\logfile"
```

Where `[path]\msifile` represents the path and name of the MSI file, and `[logpath]\logfile` represents the path and name of the output log file.

Note: To complete a silent upgrade, append the command with the `CONDITION_NOUI=1` parameter.

Note: Be aware that the `/qn` and `/qb` modes are not supported while upgrading from version 11.0.x to version 11.1.x. In this scenario, use the `CONDITION_NOUI=1` parameter instead. However, if you are upgrading from version 11.1.x to a later version, you must use the `/qn` and `/qb` modes.

8 (Optional) You can specify the following additional command line parameter to the upgrade command to stop the installation or upgrade in case of any pending restart on the system:

```
PRE_INSTALL_REBOOT_CHECK=YES
```

9 When prompted, close the **Command Prompt** window and restart the computer.

Note: If the Autologon Utility was installed on the client computer, you must also upgrade the Autologon Utility as well. To upgrade the Autologon Utility, run the `autologon msi` that you created after upgrading the Autologon snap-in on the Symantec Endpoint Encryption Management Server. When the upgrade is complete, restart the client computer.

10 Depending on the previous version of the client, do one of the following:

On **11.X.X** computers:	If you have Drive Encryption with Opal v2 compliant drives, complete the steps in the section, *Upgrading Drive Encryption with Opal v2 compliant drives*.
On **8.2.1** computers	8.2.1 - If you upgrade to the Removable Media Encryption feature, you should be able to use the normal authentication method to access the data that was previously encrypted by Removable Storage.

Upgrading Drive Encryption with Opal v2 compliant drives

If you have existing Opal v2 compliant drives that are already encrypted by Symantec Endpoint Encryption, during upgrade those drives are not converted automatically from drives that are

software encrypted to drives that are hardware encrypted. You must follow this procedure to manually convert the drives.

For more information on the Drive Encryption policy options, see the Symantec Endpoint Encryption Management Server online Help.

If the drive meets the qualifying conditions and the drive is successfully provisioned, the drive is hardware encrypted. It displays a status of “Hardware Encrypted" in reports and in the consoles. If the qualifying conditions are not met or if provisioning fails, the drive is software encrypted by Drive Encryption, and the encryption status is "Encrypted."

The type of encryption on a client computer affects how some policies are handled:

- When drives are hardware-encrypted, the policy options on the Drive Encryption - Encryption policy, such as the encryption strength or inclusion of unused disk space, are not applicable.
- If a drive is software encrypted when the Drive Encryption - Self-Encrypting Drives policy is deployed, the policy is ignored on the client computer.

To move an Opal v2 compliant drive from software encryption to hardware encryption, after you upgrade to Symantec Endpoint Encryption to 11.2.0:

1. Prerequisites:
   - Make sure that the drive appears on the whitelist of supported Opal drives.
     List of Opal v2 Compliant Drives
   - If the drive is a Microsoft eDrive support - Opal v2 compliant drive, verify the drive's partitions. Make sure that:
     - The default partitions were created during a default Microsoft Windows installation, and
     - When multiple partitions exist, the number of ranges is properly mapped to the number of partitions.
2. Decrypt the drive using Symantec Endpoint Encryption. To issue decrypt commands, do the following:
   - From the Management Server, use the Server Commands snap-in, or
   - From the client computer, ask a client administrator to use either the Drive Encryption Administrator Command Line or the Client Administrator Console.
3. Configure and deploy the Drive Encryption - Self-Encrypting Drives install-time, GPO, or native policy, with the **Use hardware encryption for compatible Opal-compliant drives** option enabled.
4. Re-issue an encrypt command from Symantec Endpoint Encryption. To issue encrypt commands, do the following:
   - From the Management Server, use the Server Commands snap-in, or

- From the client computer, ask a client administrator to use either the Drive Encryption Administrator Command Line or the Client Administrator Console.

The encrypt command recognizes the Opal v2 compliant drive and attempts to manage and secure the drive. If a drive is not provisioned in Single User Mode, Drive Encryption provisions it in Global Range Mode.

Updating the existing GPO or native BitLocker Client policies post upgrade

After you upgrade the Symantec Endpoint Encryption Management Server and Manager Console to version 11.1.2 or later, as a best practice, revisit the BitLocker client policies for encryption (Encryption and Authentication policy) and client lockout (Client Monitor policy). Note that the BitLocker client GPO and native policies are also now available as an install-time policy in versions 11.1.2 and later.

Upgrading the Autologon Utility

After you upgrade the Drive Encryption feature, you must upgrade the Autologon Utility. To upgrade the Autologon Utility, you must create a new Autologon Utility installation package and deploy it on the client computer. When the upgrade is complete, restart the client computer.

Installing additional client features after upgrading

Optionally, after you complete the upgrade to version 11.2.0, you can install additional features that were not previously enabled. For example, after you finish upgrading Drive Encryption, you can install Removable Media Encryption on the client computers.

To install additional features, you must create a new Symantec Endpoint Encryption Client installation package that has the new feature enabled. Be aware that some features cannot co-exist with other features.

See "About enabling features in the Symantec Endpoint Encryption Client installation package" on page 66.

When you are ready, deploy the new Symantec Endpoint Encryption Client installation package using the following command:

```
MSIEXEC /i "[path]\msifile" REINSTALLMODE=vemus ADDLOCAL=ALL /l*v
"[logpath]\logfile"
```

Where `[path]\msifile` represents the path and name of the MSI file, and `[logpath]\logfile` represents the path and name of the output log file.

When the installation is complete, restart the client computer.

Note: When you upgrade the Symantec Endpoint Encryption Client, you must also upgrade any additional features that are installed, such as the Autologon Utility and the Windows Password Reset Utility.

Using Group Policy Objects when upgrading Microsoft Windows clients

While upgrading clients to Symantec Endpoint Encryption 11.2.0, you can use a GPO to distribute the Symantec Endpoint Encryption Client installation package to the computers in your organization.

When you deploy Symantec Endpoint Encryption Client 11.2.0 on a Microsoft Windows computer, the installer performs one of the following actions:

- If you upgrade from Symantec Endpoint Encryption 11.x, the existing features are upgraded, and additional features are installed if they are enabled in the MSI file.
- If you upgrade from Symantec Endpoint Encryption 8.2.1, the Framework, Full Disk and Removable Storage clients are uninstalled. Symantec Endpoint Encryption Client is installed without decrypting the disk.
- If you upgrade from Symantec Encryption Desktop 10.3.2 MP4, MP9, MP10, or MP11, only the Symantec Drive Encryption feature is disabled. Symantec Endpoint Encryption Client is installed without decrypting the disk, and no other Symantec Encryption Desktop features are disabled. If required, you can uninstall Symantec Encryption Desktop later.

Note: If the currently installed version of the Symantec Endpoint Encryption client software was deployed using a GPO, before you upgrade to version11.2.0, update the GPO to remove the original MSI file. Make sure that you do not select the option to uninstall the client software when you update the GPO.

Tailor the following procedures to suit the requirements of your organization.

Creating Symantec Endpoint Encryption Client installers for distribution

To create Symantec Endpoint Encryption client installers for distribution

- Create the MSI file for Symantec Endpoint Encryption Client. Choose the 32-bit or 64-bit version, as appropriate for the version of Microsoft Windows installed on your client computers.

  Note: If you upgrade a client using a Symantec Endpoint Encryption Client installation package that was created using a different Symantec Endpoint Encryption Management Server, the Help Desk Recovery feature stops working as the client computer does not exist in the new server's database. After the upgrade is complete, ensure that the client checks in with Symantec Endpoint Encryption Management Server. Then, disable and re-enable the Help Desk Recovery feature through the policy settings.

For more information about creating the Symantec Endpoint Encryption Client installation package, see the *Creating Symantec Endpoint Encryption client installers* chapter available in the *Symantec Endpoint Encryption Management Server Online Help*.

See "Creating a Symantec Endpoint Encryption Client installation package" on page 48.

Creating an Active Directory distribution point

To create a distribution point on your Active Directory forest or domain

1. Save the created MSI file that you want to deploy using a GPO in a folder that is in a shared network location. For example, the location can be the domain controller's SYSVOL folder. The created folder is the distribution point on your Active Directory forest or domain.
2. Set the folder properties to enable users to have read and execute permissions. For example, you can avoid access permission issues during deployment if you set the security property of the shared folder to **Everyone**.

Caution: Carefully review your procedures on your network and follow the rights assignment policies of your organization. Reset the security property of the shared folder immediately when you finish deployment.

Creating an upgrade script file

Create a startup script to run the following command on the client computers that you want to upgrade to Symantec Endpoint Encryption 11.2.0:

```
MSIEXE /i "[path]\msifile" /norestart CONDITION_NOUI=1 /l*v "[logpath]\logfile"
```

Where `[path]\msifile` represents the share path and name of the MSI file, and `[logpath]\logfile` represents the path and name of the output log file.

Note: Refer to the sample upgrade script that is provided in the Symantec Knowledge Base article http://www.symantec.com/docs/HOWTO124269.

Creating GPOs to deploy the upgrade script

To create Group Policy Objects and deploy the upgrade script

Note: If User Account Control (UAC) is enabled on a client computer, you must enable the **Always install with elevated privileges** group policy setting under **Computer Configuration** and **User Configuration** in the **Group Policy Management Editor**.

---

1. Open **Symantec Endpoint Encryption Management Console**.
2. In the left pane, expand **Group Policy Management**.

3 Right-click **Group Policy Objects** and click **New**.

4 In the **New GPO** window, type a GPO title in the **Name** box and click **OK** to save the new policy.

Note: Each MSI must have its own GPO. Ensure that you create separate GPOs for 32-bit and 64-bit packages.

5 Right-click the created GPO, and select **Edit**.

6 In the left pane of the **Group Policy Management Editor**, navigate to **Computer Configuration > Policies > Windows settings > Scripts (Startup/Shutdown)**.

7 In the right pane, double-click **Startup**.

8 On the **Scripts** tab of the **Startup Properties** dialog box, click **Add**.

9 In the **Add a script** dialog box, click **Browse**.

10 Using the navigation windows to select the script file, and then click **Open**.

11 To submit the script file, click **OK**.

12 To close the **Startup Properties** dialog box, click **OK**.

13 Close the **Group Policy Management Editor**.

Installing the client installer GPOs

After you finish configuring the GPO, restart the client computers to begin the upgrade.

Note: When you upgrade the Symantec Endpoint Encryption Client, you must also upgrade any additional features that are installed, such as the Autologon Utility and the Windows Password Reset Utility.

Upgrading Symantec Endpoint Encryption for FileVault clients

Before you upgrade Symantec Endpoint Encryption for FileVault to version 11.2.0, ensure that the disk is either completely encrypted or decrypted. If encryption or decryption is in progress, wait until the disk is completely encrypted or decrypted.

To upgrade Symantec Endpoint Encryption for FileVault manually

- Double-click the Symantec Endpoint Encryption for FileVault installation package file.

To upgrade Symantec Endpoint Encryption for FileVault using the command line

1. Launch the Terminal application.
2. In the Terminal window, enter the following command:

   ```
   sudo installer -package [filepath] -target /
   ```

   where, `[filepath]` represents the location and name of the Symantec Endpoint Encryption for FileVault installation package file.

Note: After the upgrade is complete, ensure that the users have secure token enabled for their account to perform FileVault operations, such as enabling, migrating, and adding users, on a system with macOS High Sierra (10.13.x) (with APFS) installed.

For information on how to enable secure token, see the Apple documentation.

Chapter 5

Using the Symantec Endpoint Encryption Management Server Configuration Manager

This chapter includes the following topics:

- Symantec Encryption Management Server page (optional)

About using the Symantec Endpoint Encryption Management Server Configuration Manager

You can use the **Symantec Endpoint Encryption Management Server Configuration Manager** to change the configuration settings of your Symantec Endpoint Encryption Management Server.

Before you log on to the Symantec Endpoint Encryption Management Server, consider the following:

- If you use Microsoft Windows authentication, log on with either the Symantec Endpoint Encryption Management Server account or the database creation account.
- If you use mixed-mode authentication, log on with an account that has local administrator rights and read and write permissions to the database.

Database Configuration page

The **Database Configuration** page lets you view and change the Symantec Endpoint Encryption database options.

Table 5-1 Options of the **Database Configuration** page

Option	Description
Database server name	This option displays the NetBIOS name of the computer that hosts the Symantec Endpoint Encryption database. If you use a named instance, this field displays the NetBIOS name and the instance name. For example, **SEEDB-01\NAMEDINSTANCE**. You should edit this option if you moved the Symantec Endpoint Encryption database to a different computer, or if you renamed the computer. **Note:** To enable TLS/SSL, this name must match the common name (CN) in the server-side TLS/SSL certificate.
Custom port	If you configured the Symantec Endpoint Encryption database to use a custom port, this field displays the port number. This field is empty if the Symantec Endpoint Encryption database uses the default port number. You should enter the new port number if you have changed the port number of the Symantec Endpoint Encryption database.

Table 5-1 Options of the **Database Configuration** page *(continued)*

Option	Description
Database name	This field displays the name of the Symantec Endpoint Encryption database.
Authentication mode	This option lets you choose how the Symantec Endpoint Encryption Management Server authenticates with the database. ■ **Windows authentication** lets you configure the Symantec Endpoint Encryption Management Server to authenticate to the database through Windows Domain authentication. ■ **SQL Server authentication** lets you configure the Symantec Endpoint Encryption Management Server to authenticate to the database through SQL authentication.
User name	Enter the user name for the account that authenticates with the database. ■ If you use Microsoft Windows authentication, this field displays the domain account that you provisioned before you installed the Symantec Endpoint Encryption Management Server. You must enter the user name *domain\user name* format. ■ If you use SQL authentication, this field displays the Microsoft SQL Server account that you created when you installed the Symantec Endpoint Encryption Management Server.
Password	■ **Password** Enter the password for the Microsoft SQL Server account or the Windows Domain account. This account is the one that the Symantec Endpoint Encryption Management Server uses to communicate with the Symantec Endpoint Encryption database. ■ **Show password** Select this option to display the characters that you type in the **Password** field. After you save your changes, the dialog displays the message, "**Changes are saved successfully**." The password characters are obfuscated with symbols.
Enable TLS/SSL	Click this option to encrypt the traffic between the Microsoft SQL Server database and the Symantec Endpoint Encryption Management Server. For more information about configuring TLS/SSL communications, see the section "About configuring TLS/SSL communications for Symantec Endpoint Encryption" in the *Symantec Endpoint Encryption Installation Guide*.
Cancel	To leave the wizard, click **Cancel**. Your settings are lost.

Table 5-1 Options of the **Database Configuration** page *(continued)*

Option	Description
Next/Save	To save your settings, click **Next** during installation or **Save** during an update.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Web Server Configuration page

The **Web Server Configuration** page lets you view and modify your Symantec Endpoint Encryption Management Server and client computer communication settings.

Table 5-2 Options of the **Web Server Configuration** page

Option	Description
Web server name	This field displays the name of the computer that hosts the Symantec Endpoint Encryption Management Server. This field displays the NetBIOS name by default but it also accepts a fully qualified domain name (FQDN). You may need to change this value under the following circumstances: ■ The computer name of the Symantec Endpoint Encryption Management Server is changed. ■ DNS configuration issues prevent the Configuration Manager from resolving the NetBIOS name. In this case, use the FQDN. **Note:** To use HTTPS communication, this name must match the common name (CN) in the server-side TLS/SSL certificate.

Table 5-2 Options of the **Web Server Configuration** page *(continued)*

Option	Description
Credentials	These fields display the name and domain of the Internet Information Services (IIS) client account. If you change the IIS client account, you must enter the credentials of this account. ■ **User name** Enter the user name for the IIS client account. ■ **Password** Enter the password for the IIS client account. ■ **Show password** Select this option to display the characters that you type in the **Password** field. ■ **Enable Windows Authentication** Select this option to distribute Removable Media Encryption workgroup key to your Active Directory computers. To enable Windows authentication, the Windows authentication server role must be selected from the **Add Roles and Feature Wizard**. After you save your changes, the dialog displays the message, "**Changes are saved successfully**." The password characters are obfuscated with symbols.
Protocol	These fields let you select your communication protocol and enter the port numbers for HTTP and HTTPS traffic. ■ **HTTP** Enter the **TCP port** on the Symantec Endpoint Encryption Management Server for unencrypted client communication. Make sure that the port number is not already in use. **Note:** You should not use the HTTP protocol unless you are deploying the Symantec Endpoint Encryption Management Server in a test environment. Use HTTPS protocol for secure communications in a production setting. ■ **HTTPS** Select this option to enable HTTPS communication. Enter the **SSL port** on Symantec Endpoint Encryption Management Server for encrypted client communication. Make sure that the port number is not already in use.

Table 5-2 Options of the **Web Server Configuration** page *(continued)*

Option	Description
Secure certificates	These fields let you provide your client-side and server-side certificates for secure communication. ■ **CA certificate** This option is the certificate that client computers use for encrypted communication with the Symantec Endpoint Encryption Management Server. The client computer uses this certificate to verify the Server certificate that the server presents during an SSL handshake. To choose the SSL certificate file, click **Browse**. Browse to the correct CA certificate and then click **Open**. The dialog box displays the certificate hash string beside the **Browse** option. ■ **Server certificate** This option is the certificate that the Symantec Endpoint Encryption Management Server uses for encrypted communication with Symantec Endpoint Encryption client computers. To choose the SSL certificate file, click **Browse**. Browse to the correct TLS/SSL certificate and then click **Open**. The dialog box displays the certificate hash string beside the **Browse** option. **Note:** Selecting the server-side TLS/SSL certificate in the **Configuration Manager** also assigns the server-side TLS/SSL certificate to the Symantec Endpoint Encryption services website. For more information about configuring TLS/SSL communications, see the section "About configuring TLS/SSL communications for Symantec Endpoint Encryption" in the *Symantec Endpoint Encryption Installation Guide*.
Cancel	To leave the wizard, click **Cancel**. Your settings are lost.
Next/Save	To save your settings, click **Next** during installation or **Save** during an update.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Active Directory Configuration page

The **Active Directory Configuration** page lets you view and change your Active Directory configuration settings. You can configure directory synchronization with multiple forests and trees. You can configure domain filtering, and also enable TLS/SSL encryption.

Table 5-3 Options of the Active Directory Configuration page

Option	Description
Add one or more AD forest	Click the **Add one more AD forest** icon (+ symbol), to synchronize with additional Active Directory forests.
Remove this AD forest	Click the **Remove this AD forest** icon ("X" symbol), to remove the configuration information for the currently displayed forest.
Active Directory forest name	This field is the name of the specified forest.
Global catalog server	(Optional) This field is the name of the global catalog server computer for the specified forest. Use the fully qualified domain name of the global catalog server.
Credentials	These fields display the name and domain of the Active Directory synchronization account. If you change the Active Directory synchronization account, you must enter the credentials of this account. ■ **User name** Enter the Domain and the user name for the Active Directory synchronization account. ■ **Password** Enter the password for the Active Directory synchronization account. ■ **Show password** Select this option to display the characters that you type in the **Password** field.
Enable TLS/SSL	This option lets you encrypt all of your synchronization traffic between Active Directory and the Symantec Endpoint Encryption Management Server. This option requires you to install and configure TLS/SSL certificates.
Configure the domain filter	This option lets you specify Active Directory domains to be included or excluded from synchronization. For example, there may be domains within your forest(s) that do not contain Symantec Endpoint Encryption client computers. To improve performance and usability, you can exclude these domains from being synchronized. To add a domain filter, click **Configure Domain Filter**. In the **Include Computers from** column, select a domain you want to exclude and click the **">>"** symbol. If you exclude a parent domain, you also exclude all child domains of that parent domain.
Cancel	To leave the wizard, click **Cancel**. Your settings are lost.
Next/Save	To save your settings, click **Next** during installation or **Save** during an update.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Active Directory Synchronization Service page

The **Active Directory Synchronization Service** page displays the options and status information for your directory service.

Directory service synchronization runs about every 15 minutes and updates the data that is different from the last synchronization such as new users or deleted computers.

Table 5-4 Options of the Active Directory Synchronization Service page

Option	Description
Status	This section displays the current status of synchronization with the directory service. A message displays the last time that you synchronized the directory. The status values are as follows: ■ **Running** The synchronization service is running. ■ **Stopped** The synchronization service is stopped. ■ **Start Pending** The synchronization service is starting. ■ **Continue Pending** The synchronization service is restarting. ■ **Pause Pending** The synchronization service is stopping.
Refresh Status	To refresh the synchronization service values, click this option.
Start	To start a stopped service, click this option.
Stop	To stop the synchronization service, click this option.
Restart	To restart the service, click this option.
Full Synchronization	This option makes the Active Directory Synchronization Service run a full synchronization. It also restarts the Active Directory Synchronization Service. The Active Directory Synchronization Service works in the background. The Full Synchronization option returns to its normal state after the Active Directory Synchronization restart operation completes. Depending on the size of your organization, this operation may take time to complete. This operation can temporarily increase the load on the Symantec Endpoint Encryption database and each directory service.

Table 5-4 Options of the Active Directory Synchronization Service page *(continued)*

Option	Description
Method	This option lets you select whether each directory synchronization service should start automatically or manually. ■ To run the service automatically at boot time, click **Automatic synchronization**. ■ If you do not want the service to run automatically at boot time, click **On-demand synchronization**.
Server type	By default, each Symantec Endpoint Encryption Management Server is installed as a primary synchronizer. When you set up multiple Symantec Endpoint Encryption Management Servers, you should only configure a single Symantec Endpoint Encryption Management Server as primary. All other Symantec Endpoint Encryption Management Servers should be configured as secondary. ■ **Primary synchronizer** Click this option to configure this Symantec Endpoint Encryption Management Server to act as a primary synchronizer. ■ **Secondary synchronizer** Click this option to configure this Symantec Endpoint Encryption Management Server to act as a secondary synchronizer.
Reverse data verification	This option ensures that all deleted directory objects are synchronized with the Symantec Endpoint Encryption Management Server. This setting is disabled by default. This setting doubles the number of times that the directory is queried for changes and can decrease network performance. You should analyze your directory synchronization network traffic before and after you enable this setting so that you can assess its effect on your network.
Cancel	To leave the wizard, click **Cancel**. Your settings are lost.
Next/Save	To save your settings, click **Next** during installation or **Save** during an update.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Novell eDirectory Configuration page

This topic is applicable only when you upgrade your server. The **Novell eDirectory Configuration** page lets you view and change your Novell eDirectory configuration settings.

Table 5-5 Options of the Novell eDirectory Configuration page

Option	Description
Add icon	Click this icon to add a Novell eDirectory tree.
Remove icon	Click this icon to remove the Novell eDirectory tree that is displayed.
Novell Tree Name	Enter the name of the Novell eDirectory tree that you want to configure.
LDAP host server IP	Enter the IP address of the LDAP server that hosts the Novell eDirectory. This server must support chaining and persistent searches to work with the Symantec Endpoint Encryption Management Server.
LDAP port	Enter the TCP port of the LDAP server that hosts the Novell eDirectory. The Symantec Endpoint Encryption Management Server uses this port for its LDAP connection.
Credentials	These fields display the name and password for your Novell eDirectory synchronization account. If you change the Novell eDirectory synchronization account, you must enter the credentials of this account. ■ **User name** Enter the user name for the Novell eDirectory synchronization account synchronization account. ■ **Password** Enter the password for the Novell eDirectory synchronization account. ■ **Show password** Select this option to display the characters that you type in the **Password** field.
Cancel	To leave the wizard, click **Cancel**. Your settings are lost.
Next/Save	To save your settings, click **Next** during installation or **Save** during an update.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Novell eDirectory Synchronization Service page

This topic is applicable only when you upgrade your server. The **Novell eDirectory Synchronization Service** page displays the options and status information about your Novell eDirectory synchronization service.

Table 5-6 Options of the Novell eDirectory Synchronization Service page

Option	Description
Status	This section displays the current status of synchronization with the directory service. A message displays the last time that you synchronized the directory. The status values are as follows: ■ **Running** The synchronization service is running. ■ **Stopped** The synchronization service is stopped. ■ **Start Pending** The synchronization service is starting. ■ **Continue Pending** The synchronization service is restarting. ■ **Pause Pending** The synchronization service is stopping. ■ **Not Installed** You have removed the service. You should only remove the synchronization service when you uninstall Symantec Endpoint Encryption.
Refresh Status	To refresh the synchronization service values, click this option.
Start	To start a stopped service, click this option.
Stop	To stop the synchronization service, click this option.
Restart	To restart the service, click this option.
Full Sync	To run a complete synchronization of all synchronization data, click this option. Depending on the size of your organization, this operation may take time to complete. This operation can temporarily increase the load on the Symantec Endpoint Encryption database and each directory service.
Method	This option lets you select whether each directory synchronization service should start automatically or manually. ■ To run the service automatically at boot time, click **Automatic synchronization**. ■ If you do not want the service to run automatically at boot time, click **On-demand synchronization**.

Table 5-6 Options of the Novell eDirectory Synchronization Service page *(continued)*

Option	Description
Server type	By default, each Symantec Endpoint Encryption Management Server is installed as a primary synchronizer. When you set up multiple Symantec Endpoint Encryption Management Servers, you should only configure a single Symantec Endpoint Encryption Management Server as primary. All other Symantec Endpoint Encryption Management Servers should be configured as secondary. ■ **Primary synchronizer** Click this option to configure this Symantec Endpoint Encryption Management Server to act as a primary synchronizer. ■ **Secondary synchronizer** Click this option to configure this Symantec Endpoint Encryption Management Server to act as a secondary synchronizer.
Reverse data verification	This option ensures that all deleted directory objects are synchronized with the Symantec Endpoint Encryption Management Server. This setting is disabled by default. This setting doubles the number of times that the directory is queried for changes and can decrease network performance. You should analyze your directory synchronization network traffic before and after you enable this setting so that you can assess its effect on your network.
Cancel	To leave the wizard, click **Cancel**. Your settings are lost.
Next/Save	To save your settings, click **Next** during installation or **Save** during an update.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Community Quality Program page

The **Community Quality Program** page lets you opt in or opt out of submitting anonymous system and product information about how you use this product to Symantec. You may opt in or opt out at any time.

See "About Symantec's Community Quality Program" on page 13.

Information purpose, type and use

The purpose of the information that is collected is to help Symantec analyze and improve the functionality of its endpoint security solutions. Such information may be comprised of installation information, software diagnostics, and facts in other pertinent categories. The data may include

general usage statistics, server load, whether client software is up to date, problems in the client profile, and general security profiles.

Data collection and transmission

Symantec Endpoint Encryption Management Server periodically sends this data to a Symantec server using SSL encryption. Data transmission takes place weekly. This information is collected anonymously. The information that is collected cannot be tracked to a specific user or customer. No new information is gathered. The information already exists in your database.

When you opt in, data transmission is scheduled immediately. When you opt out, data transmission stops; transmission is no longer scheduled.

Table 5-7 Options of the Community Quality Program tab

Option	Description
Participate in Symantec's Community Quality Program	(default) To opt in to the program, check the **Participate in Symantec's Community Quality Program** check box. To opt out of the program, uncheck the check box. If you opt-in to the program, the current server is configured to transmit telemetry data. If you have a clustered deployment, the telemetry transmissions are only done by the most recently configured Symantec Endpoint Encryption Management Server.
Cancel	To leave the wizard, click **Cancel**. Your settings are lost.
Next/Save	To save your settings, click **Next** during installation or **Save** during an update. **Note:** If you receive the following error message, contact your SQL server administrator to troubleshoot the issue: ""Unable to access Symantec Endpoint Encryption Management Server data store for the Community Quality Program. The Telemetry Credentials are invalid or SQL Server authentication has failed. To resolve this issue, contact your database administrator." **Note:** For more information about troubleshooting telemetry settings, see the following Symantec Knowledgebase article: http://www.symantec.com/docs/HOWTO110233

See “About using the Symantec Endpoint Encryption Management Server Configuration Manager” on page 91.

About Administrative Server Roles

The Symantec Endpoint Encryption Configuration Manager lets you assign Symantec Endpoint Encryption Management Server roles to an individual administrative user or a group of administrative users. You can assign these roles to an administrative user or a group of administrative users and provide application-level access and allow administrative users to access only certain server snap-ins, such as Help Desk.

As of version 11.2, Symantec Endpoint Encryption lets you assign one more endpoint groups to an individual administrative user or a group of administrative users. Endpoint groups are created when you configure organizational units (OUs) in Microsoft Active Directory. When you assign an endpoint group to an individual administrative user or a group of administrative users, the scope of some of their privileges becomes restricted so that their actions affect only the client computers that are a part of the assigned endpoint group.

By default, when you upgrade to version 11.2 or later, all administrative users and groups that have an assigned server role have control over all existing endpoint groups.

Note: Endpoint group-level restrictions affect only administrative actions that are performed on client computers in Microsoft Active Directory. Administrative actions that are performed on native client computers are not restricted by the administrative users' or groups' assigned endpoint groups.

The server roles are as follows:

- **Server** - Unaffected by endpoint group assignment.
- **Setup** - Unaffected by endpoint group assignment.
- **Policy** - Some administrative user actions are restricted to only the users' assigned endpoint groups.
- **Report** - Unaffected by endpoint group assignment.
- **Help Desk** - Some user actions are restricted to only the users' assigned endpoint groups.

Server Role functions

The following table lists the server roles and the Management Console snap-ins to which each server role allows access. The table also lists a summary of the functions that an administrator can perform with each snap-in.

Table 5-8 Server Role functions

Server Role	Snap-in Access	Function
Server	Symantec Endpoint Encryption Management Password All other snap-ins as listed below	Set up and change the Management Password. The Management Password is required to: ■ Install and upgrade Symantec Endpoint Encryption Management Server ■ Install and upgrade the Management Console ■ Access the Help Desk Recovery snap-in in the Management Console ■ Create the Autologon utility installation package ■ Create the Windows Password Reset Utility installation package If the Management Password is lost, the Management Server must be reinstalled.
	Symantec Endpoint Encryption Database Maintenance	View and remove old tracked endpoints and recorded client events from the database.
Setup	Symantec Endpoint Encryption Software Setup	Create installation policies for the Management Agent, Drive Encryption, and Removable Media Encryption and generate client MSIs.
	Symantec Endpoint Encryption Autologon Utility	Generate MSIs that enable or disable the autologon function on client computers. If autologon is enabled, users bypass preboot authentication.
	Symantec Endpoint Encryption Windows Password Reset	Generate the Windows Password Reset Utility MSI that installs the Windows Password Reset feature on Drive Encryption client computers.

Table 5-8 Server Role functions *(continued)*

Server Role	Snap-in Access	Function
Policy	Symantec Endpoint Encryption Native Policy Manager	Create and deploy native policies to client computers in the administrative user's assigned endpoint groups.
	Active Directory Users and Computers	Manage users and computers in the AD hierarchy.
	Symantec Endpoint Encryption Users and Computers	Manage users and computers in the SEE hierarchy.
	Group Policy Management	Create and deploy GPOs to client computers. To access group policy management snap-ins without any issue, the user should be a member of the following four security groups: 1 Domain Administrators 2 Domain Users 3 Enterprise Administrators 4 Group Policy Creator owners
	Symantec Endpoint Encryption Server Commands	

Table 5-8 Server Role functions *(continued)*

Server Role	Snap-in Access	Function
		Issue server-based commands from the Symantec Endpoint Encryption Users and Computers snap-in. The commands are to encrypt or decrypt fixed disk drives on specified client computers in the administrative user's assigned endpoint groups. The Symantec Endpoint Encryption Server Commands snap-in provides reports on issued commands. It also provides an interface for canceling pending commands. **Note:** In the Management Console, administrative users who have the Policy Administrator server role can issue server commands only to the client computers that belong to their assigned endpoint groups. Server command-related options in the Management Console appear greyed out for client computers that do not belong to the administrative user's assigned endpoint groups.

Table 5-8 Server Role functions *(continued)*

Server Role	Snap-in Access	Function
Report	Symantec Endpoint Encryption Reports	Run and customize predefined reports for client computers. View information about client computers, Active Directory and native policy settings, and Active Directory service synchronization. To access custom reports, the user must have administrative rights. Local users cannot access custom reports. **Note:** Users with the Report Administrator server role might not be able to issue server-based commands from within reports, depending on whether they also have the Policy role and the necessary endpoint groups assigned to them.
Help Desk	Symantec Endpoint Encryption Help Desk	Use online or offline Help Desk recovery options to assist users to regain access to their computers from preboot, either because of a forgotten password or a computer lockout. **Note:** If a Microsoft Windows computer was encrypted using either Symantec Endpoint Encryption Drive Encryption or Symantec Endpoint Encryption for BitLocker, you can provide recovery assistance only if that computer belongs to one of the endpoint groups that are assigned to you.

See "Server Roles Configuration page" on page 113.

Configuring Server Roles

You can define server roles for individual Active Directory administrative users and user groups and for local administrative users and user groups. You can define the database access to users and groups and you can limit administrative access in the Management Console. This feature can be enabled or disabled by the server administrator. When you enable this feature, the logged in user is added as the Server Administrator role and has access to all snap-ins, and all endpoint groups are assigned to the user.

To configure server roles for Active Directory users:

1. On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.
2. Select **Server Roles** from the list on the left of the screen.
3. On the **Server Roles Configuration** page, switch the **Manage Server Roles** toggle to **On**.
4. Click **Allow Symantec Endpoint Encryption to manage database access permissions for AD users** to enable Symantec Endpoint Encryption to configure and manage SQL server logins and database access permissions for Active Directory users.

   Note: Make sure that the user who authenticated to the database has the appropriate roles and permissions to manage SQL Server database users.

5. Do one of the following:
   - Click **Add User** to add and configure one or more server roles to an Active Directory user.
   - Click **Add Group** to add and configure one or more server roles to a group of Active Directory users.
6. Under **Select location**, browse to the Active Directory users.

   Note: The **Select location** pane enables you to navigate only the domain that the Symantec Endpoint Encryption Management Server belongs to. If your organization owns multiple domains, you must configure server roles on each domain's Symantec Endpoint Encryption Management Server separately.

7. On the **Select User** page or the **Select Group** page, enter a partial user name or group name in the search box.

8 Click **Search**.

Note: You can use the % character or the * character to perform a wild card search a partial name.

9 Select one or more users or groups from the list.

Note: You can repeat the search for multiple user names or group names. This enables you to configure the same server roles for multiple users or groups simultaneously.

10 Click **Show Selected** to view the list of users or groups that you selected for configuration.

11 Click **Next**.

12 On the **Map Endpoint Groups** page, do one of the following:

- To assign control over all existing endpoint groups to the selected Active Directory users or groups, select **All Endpoint Groups**.
- To assign control over specific endpoint groups to the selected Active Directory users or groups, select **Selective Endpoint Groups**.
  Then, in the search box, enter a partial endpoint group name and click **Search**. In the search results, select the endpoint groups that you want to assign to the selected users or groups.
  You can click **Show Selected** to view the list of endpoint groups that will be assigned to the selected users or groups.

  Note: You can repeat the search for multiple endpoint group names.

13 Click **Next**.

14 On the **Map Admin Roles** page, to assign one or more roles to one or more selected Active Directory users or groups, select one or more check boxes next to the displayed roles.

Note: To actively deny all administrative privileges to specific users, leave all of the server roles unselected for those users. As server role configurations for individual users supercede the server role configurations for groups, the specified users are denied all administrative privileges even if they belong to one or more groups that are configured with server roles.

15 Click **Next**.

16 On the **Summary** page, review the configured settings, and then click **Finish**.

17 On the **Server Roles Configuration** page, click **Save**.

To configure server roles for Local Users:

1 On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.

2 Select **Server Roles** from the list on the left of the screen.

3 On the **Server Roles Configuration** page, switch the **Manage Server Roles** toggle to **On**.

4 Do one of the following:

- Click **Add User** to add and configure one or more server roles to a local user.
- Click **Add Group** to add and configure one or more server roles to a group.

5 Under **Select location**, select **This Computer**.

6 On the **Select User** page or the **Select Group**, click **Search** to view a list of all available local users or local groups.

7 Click **Search**.

8 Select one or more users or groups from the list.

Note: You can repeat the search for multiple user names or group names. This enables you to configure the same server roles for multiple users or groups simultaneously.

---

9 Click **Show Selected** to view the list of users or groups that you selected for configuration.

10 Click **Next**.

11 On the **Map Endpoint Groups** page, do one of the following:

- To assign control over all existing endpoint groups to the selected users or groups, select **All Endpoint Groups**.
- To assign control over specific endpoint groups to the selected users or groups, select **Specific Endpoint Groups**.
  Then, in the search box, enter a partial endpoint group name and click **Search**. In the search results, select the check box that corresponds to the endpoint groups that you want to assign to the selected users or groups.

Note: You can repeat the search for multiple endpoint group names.

---

12 Click **Show Selected** to view the list of endpoint groups that will be assigned to the selected users or groups.

13 Click **Next**.

14 On the **Map Admin Roles** page, to assign one or more roles to one or more selected users or group, select one or more check boxes next to the displayed roles.

Note: To actively deny all administrative privileges to specific users, leave all of the server roles unselected for those users. As server role configurations for individual users supercede the server role configurations for groups, the specified users are denied all administrative privileges even if they belong to one or more groups that are configured with server roles.

---

15 Click **Next**.

16 On the **Summary** page, review the configured settings, and then click **Finish**.

17 On the **Server Roles Configuration** page, click **Save**.

Editing configured Server Roles

The server administrator can edit existing server role configuration records to modify the assigned endpoint groups and assigned server roles.

To edit configured server roles:

1 On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.

2 Select **Server Roles** from the list on the left of the screen.

3 On the **Server Roles Configuration** page, select the server role configuration record that you want to modify.

4 Click **Edit**.

5 On the **Map Endpoint Groups** page, do one of the following:

- To assign control over all existing endpoint groups to the user or group in the record, select **All Endpoint Groups**.
- To assign control over specific endpoint groups to the user or group in the record, select **Selective Endpoint Groups**.
  Then, in the search box, enter a partial endpoint group name and click **Search**. In the search results, select the endpoint groups that you want to assign to the user or group.
  You can click **Show Selected** to view the list of endpoint groups that will be assigned to the user or group.

Note: You can use the % character or the * character to perform a wild card search using a partial name.

6 Click **Next**.

7 On the **Map Admin Roles** page, to assign one or more roles to the user or group in the server role configuration record, select one or more check boxes next to the displayed roles.

Note: To actively deny all administrative privileges to a specific user, leave all of the server roles unselected for those users. As server role configurations for individual users supercede the server role configurations for groups, the specified users are denied all administrative privileges even if they belong to one or more groups that are configured with server roles.

8 Click **Next**.

9 On the **Summary** page, review the changed settings, and then click **Finish**.

10 On the **Server Roles Configuration** page, click **Save**.

Disabling Server Roles

The server administrator can disable the Server Roles feature at any time so that all users running the Configuration Manager have access to all snap-ins. Once this feature is disabled, the user accounts are removed from the user interface but are not deleted from the database. If you re-enable the Server Roles feature, the previously assigned users are available.

To disable the Server Roles feature:

1 On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.

2 Select **Server Roles** from the list on the left of the screen.

3 Change the **Manage Server Roles** toggle button to the **Off** position.

4 Click **Save**.

Note: When the Configuration Manager is launched and server roles are enabled, the current user is automatically assigned to the server administrator role and is assigned control over all endpoint groups. This user can modify all other users and groups but cannot change their own server role configuration record.

Server Roles Configuration page

The Symantec Endpoint Encryption Configuration Manager lets you choose from multiple administrative server roles to provide application-level access control. You can assign these roles to administrative users and provide access to only certain server snap-ins, such as Help Desk.

In Active Directory, you can create server administrator groups, and then use the Configuration Manager to assign group-based roles. You can create groups of server administrators who require similar administrative access permissions, then assign the appropriate server roles to each group. Some roles grant restricted privilege so that actions performed by administrative users affect only the their assigned endpoint groups.

For more information about adding, editing, configuring, and removing server roles, see the topic "Essential administration tasks" in the Symantec Endpoint Encryption Management Server Online Help.

Table 5-9 Options of the Server Roles Configuration page

Option	Description
Manage Server Roles	Enable this option to add, remove, and edit your server roles.
Add User	Click this option to add and configure a new server role to a user. Launches the **Add User / Groups** wizard.
Add Group	Click this option to add and configure a new server role to a group. Launches the **Add User / Groups** wizard.
Users/Groups column	Displays the names of the users and groups that have been configured
Role columns	Each column indicates the assignment status of that particular server role for the corresponding user record or group record. ■ A red dot indicates that the server role has not been assigned to the corresponding user or group. ■ A green dot indicate that the server role has been assigned to the corresponding user or group
Endpoint Groups	Indicates either that the user or group has administrative control over all existing endpoint groups, or indicates the number of endpoint groups that are assigned.

Table 5-9 Options of the Server Roles Configuration page *(continued)*

Option	Description
Actions column	Enables you to perform the following actions: 1 To edit the assigned server roles or change the assigned endpoint groups for a user or group, click the Edit button in the corresponding record. 2 To delete a user or group from the list of configured users and groups, click the Delete button in the corresponding record. This also revokes all server roles for that particular user or group.
Allow Symantec Endpoint Encryption to manage database access permissions for AD users	Click this option to enable Symantec Endpoint Encryption to configure and manage SQL server logins and database access permissions for Active Directory users. **Note:** Before enabling this option ensure the user who authenticate to the database have appropriate roles and permissions to manage SQL Server database users.
Save	After you complete the **Add Users / Groups** wizard, click **Save** to save the newly created or modified server roles configuration.
Cancel	To discard your changes to the server roles configuration, click **Cancel**.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Symantec Encryption Management Server page (optional)

The **Symantec Encryption Management Server** page lets you configure one or more Symantec Encryption Management Server servers. This feature lets you use a single web Help Desk Recovery console for the recovery of clients reporting to different Symantec Encryption Management Servers using a whole-disk recovery token (WDRT).

Table 5-10 Symantec Encryption Management Server page

Option	Description
The plus sign (**+**) (Tooltip text: Add one or more Symantec Encryption Management Server)	Click the **Add one or more Symantec Encryption Management Server** icon to add a new Symantec Encryption Management Server. The icon is available beside **Manage Symantec Encryption Management Server**.

Table 5-10 Symantec Encryption Management Server page *(continued)*

Option	Description
The cross sign (**x**) (Tooltip text: Remove this Symantec Encryption Management Server)	Click the **Remove this Symantec Encryption Management Server** icon to remove a specific Symantec Encryption Management Server. To view this icon, expand the Symantec Encryption Management Server that you want to delete.
Server Hostname/IP	Enter the host name or IP address of the Symantec Encryption Management Server.
Password authentication	■ **User name** Enter the administrator name to be used to connect to the Symantec Encryption Management Server. This administrator must have WDRT privileges. ■ **Password** Enter the administrator password to be used to connect to the Symantec Encryption Management Server. ■ **Show password** Select this option to view the password characters as you type in the **Password** field.
Test connection	Click **Test Connection** to verify if the Symantec Endpoint Encryption Management Server can establish connection with the newly configured Symantec Encryption Management Server. If the connection is not properly configured, an error message appears that indicates the reason.
Cancel	To close the **Symantec Encryption Management Server** page, click **Cancel**. Your settings are lost.
Next/Save	To save your server configuration settings, click **Next** during installation, or **Save** during an update.

See "About using the Symantec Endpoint Encryption Management Server Configuration Manager" on page 91.

Chapter 6

Certificates and Token Software Settings

This chapter includes the following topics:

Using Symantec Endpoint Encryption authentication certificates

About certificate issuance from Windows Server 2003

If Windows Server 2003 is the operating system for the certificate authority computer, download and apply the following Microsoft patch before issuing certificates:

http://www.microsoft.com/downloads/details.aspx?FamilyId=FFAEC8B2-99E0-427A-8110-2F745059A02D&displaylang=en

Best practices: placing a single certificate on each token

Having multiple certificates on one token is cumbersome and potentially introduces human error. Multiple certificates that satisfy key usage and extended key usage requirements on a single token can cause user prompts. The prompts appear each time a user logs on to the Management Agent. Make sure, therefore, that only one certificate with the required key usage and extended key usage exists on each token.

Required key usage

Set the key usage on the certificate to be used for authentication to Symantec Endpoint Encryption as described in the table.

Table 6-1 Required Key Usage for Symantec Endpoint Encryption Authentication Certificates

Token type	Name	Also known as
Personal Identity Verification (PIV)	digitalSignature	Digital signature

Note: Additional key usages do not prevent a certificate from being used for authentication.

Required extended key usage

Set the extended key usage (sometimes called "enhanced key usage") on the certificate to be used for authentication to Symantec Endpoint Encryption as described in the table.

Table 6-2 Required Extended Key Usage for Symantec Endpoint Encryption Authentication Certificates

Token type	OID (object identifier)	Name	Also known as
Personal Identity Verification (PIV)	1.3.6.1.5.5.7.3.2	clientAuth	Client authentication

Note: Additional extended key usages do not prevent a certificate from being used for authentication.

See "Recommended token software configuration" on page 118.

Using Removable Media Encryption certificates

About using Removable Media Encryption certificates

The certificate to be used for file encryption or decryption must reside within the local Windows certificate store. The user can:

- Manually import the certificate into the local certificate storage
- Insert the token that contains the certificate into the computer and provide the PIN, if prompted

Required key usage

Set the key usage on the certificate to be used for file encryption or decryption as described in the table.

Table 6-3 Required Key Usage for Removable Media Encryption Certificates

Name	Also known as
keyEncipherment	Key encipherment

Without the required key usage setting:

- The certificate is not available for user selection
- Administrators cannot create client installation packages or the policies that contain Recovery Certificates

Note: Additional key usages do not prevent a certificate from being used for encryption or decryption.

See "Recommended token software configuration" on page 118.

Recommended token software configuration

Configure the token software:

- To insert the certificate into the Windows certificate store upon user logon or token insertion
- To remove the certificate from the Windows certificate store upon user logoff or token removal
- To disallow PIN caching

Note: If you allow PIN caching, users can gain access to the Management Agent even after they provide an invalid PIN.

See "Using Symantec Endpoint Encryption authentication certificates " on page 116.

See "Using Removable Media Encryption certificates" on page 117.

Chapter 7

Uninstalling Symantec Endpoint Encryption

This chapter includes the following topics:

Uninstalling the Symantec Endpoint Encryption Suite

To uninstall the Symantec Endpoint Encryption Suite:

1. Log on to the Symantec Endpoint Encryption Management Server with a domain account that has privileges to uninstall software and system administrator privileges on the Microsoft SQL Server.

   Alternatively, you can log on with a local account that has sufficient privileges to uninstall the software and then provide credentials of a Microsoft SQL account that has administrative privileges to the database.

2. Do one of the following:

   - On Windows 2012, click **Start > Settings > Control Panel > Programs and Features**.
   - On Windows 2008, click **Start**, and then click **Control Panel**. Click **Programs and Features**.

3. (Optional) If **Symantec Endpoint Encryption Autologon Client** and **Windows Password Reset Utility** are also listed in the **Programs and Features** window, then select them and click **Uninstall**.

4. In the **Programs and Features** window, select **Symantec Endpoint Encryption Suite**. Click **Uninstall**.

5. In the warning dialog box, click **Yes**.

6. In the **Symantec Endpoint Encryption Suite** dialog box, do one of the following:

   - To preserve the existing database and communication account, do not click **Delete my Management Database and SQL User account**. This option lets you reuse these if you reinstall the Symantec Endpoint Encryption Management Server later. The wizard uses the current Windows account to uninstall the Symantec Endpoint Encryption Management Server.
   - To delete the Symantec Endpoint Encryption database and database communication account, click **Delete my Management Database and SQL User account**.
     If the Windows account you logged on with has administrative privileges to the database, leave Windows authentication at the default state. Otherwise, click **SQL authentication** and enter the credentials of a Microsoft SQL account that has administrative privileges to the database.

7. Click **Next**.

Note: The wizard uninstalls the complete Symantec Endpoint Encryption Suite. That is all the features and snap-ins that were installed using the Symantec Endpoint Encryption Suite are uninstalled.

To uninstall the Symantec Endpoint Encryption Suite through command-line

- Run the following command:

```
MSIEXEC /x "[path]\SEE Server Suite x64.msi /l*v "[logpath]\logfile"
```

About repairing or modifying the Symantec Endpoint Encryption Suite installation

Symantec Endpoint Encryption does support modifying its installation from the Microsoft Windows Add/Remove programs list. However, Symantec Endpoint Encryption does not support repairing its installation from the Microsoft Windows Add/Remove programs list.

About uninstalling the Symantec Endpoint Encryption client

When you uninstall Symantec Endpoint Encryption from client computers, you can either uninstall specific features separately or uninstall all of the features together.

Note: While uninstalling features separately, you can specify only Drive Encryption, Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption. The Management Agent is removed automatically when there are no other features left to uninstall.

You can uninstall Symantec Endpoint Encryption in the following ways:

- Using a third-party tool to execute an uninstallation script on the client computers
- Using a GPO
- Using the Control Panel in Microsoft Windows
- Using the Command Prompt

Note: The uninstallation of specific features is possible only from the Command Prompt or by using a third-party tool with an uninstallation script.

Prerequisites

Before you uninstall the Drive Encryption feature:

- Make sure that all fixed disks are fully decrypted.
- (Optional) Make sure that the Autologon feature is uninstalled.
- (Optional) Make sure that the Windows Password Reset Utility is uninstalled.

Before you uninstall the Symantec Endpoint Encryption for BitLocker feature:

- On encrypted systems, ensure that the users back up their BitLocker Recovery Key for recovery. Symantec Endpoint Encryption Management Server does not store the BitLocker Recovery Key after the Symantec Endpoint Encryption for BitLocker client is uninstalled from the system. Encrypted systems can be uninstalled without being decrypted.

Note: If Symantec Endpoint Encryption manages this computer, you should manually delete it from the Management Console after you uninstall.

See "About uninstalling the Symantec Endpoint Encryption client with a third-party tool" on page 122.

See "About uninstalling the Symantec Endpoint Encryption client software using Group Policy Objects" on page 123.

See "Uninstalling the Symantec Endpoint Encryption client software using the Control Panel" on page 126.

See "Uninstalling the Symantec Endpoint Encryption client software using the command line" on page 127.

About uninstalling the Symantec Endpoint Encryption client with a third-party tool

You can uninstall the Symantec Endpoint Encryption Client package using any third-party deployment tool that supports the MSI format.

Note: Make sure that the client computers fulfill the uninstallation prerequisites before you attempt to uninstall Symantec Endpoint Encryption Client.

For large-scale deployments, you can use the command line as a basis for scripted uninstalls.

For example, you can create a batch file to invoke the Windows Installer (`msiexec.exe`). This batch file can contain one or more of the following commands:

- To uninstall the Drive Encryption feature:
  ```
  MSIEXEC /i "[path]\msifile" REMOVE="DE" /l*v "[logpath]\logfile"
  ```
- To uninstall the Symantec Endpoint Encryption for BitLocker feature:
  ```
  MSIEXEC /i "[path]\msifile" REMOVE="BL" /l*v "[logpath]\logfile"
  ```
- To uninstall the Removable Media Encryption feature:
  ```
  MSIEXEC /i "[path]\msifile" REMOVE="RME" /l*v "[logpath]\logfile"
  ```

- To uninstall the all of the Symantec Endpoint Encryption features together:

```
MSIEXEC /x "[path]\msifile" /l*v "[logpath]\logfile"
```

Where `[path]\msifile` represents the path and name of the MSI file, and `[logpath]\logfile` represents the path and name of the output log file.

Note: If you want to uninstall Symantec Endpoint Encryption Client from both 32-bit and 64-bit computers, make sure that the commands specify the appropriate MSI files.

About uninstalling the Symantec Endpoint Encryption client software using Group Policy Objects

If you used a Group Policy Object to deploy Symantec Endpoint Encryption clients, you must use the same GPO to uninstall them.

Note: You should never manually uninstall GPO-deployed client packages either manually or from the command line.

The uninstallation process consists of the following steps:

1. If you used a GPO to deploy the Drive Encryption feature, issue a server command to decrypt all of the fixed drives on all of the targeted computers.
2. If you used a GPO to deploy the Removable Media Encryption feature, manually decrypt all of the files on the removable drives that do not contain the Removable Media Access Utility.
3. Uninstall the desired features, or all of them.

Depending upon the way in which you deployed Symantec Endpoint Encryption 11.2.0, there are two ways to uninstall the clients using GPOs:

- Completely uninstall the Symantec Endpoint Encryption Client package from all of the client computers by removing the MSI file from the GPO. This method is available only if you installed Symantec Endpoint Encryption 11.2.0 directly, for example, you did not use a GPO to upgrade to version 11.2.0.
- Deploy an uninstallation script to remove the desired features, or all of them. This method is available only if you used a GPO to upgrade to Symantec Endpoint Encryption 11.2.0 from an earlier product.

As a best practice, you should set the appropriate Microsoft Windows policies to prevent users from manually removing the client packages.

Note: Uninstallation fails if all drives are not fully decrypted.

See "Uninstalling the Symantec Endpoint Encryption Client installation package using Group Policy Objects" on page 124.

See "Deploying uninstallation scripts using Group Policy Objects" on page 125.

Uninstalling the Symantec Endpoint Encryption Client installation package using Group Policy Objects

Uninstall the GPO-managed client installation package when you want to uninstall all of the Symantec Endpoint Encryption features at the same time. You can use this uninstallation method only if you used a GPO to install Symantec Endpoint Encryption 11.2.0 directly, and have not upgraded from an earlier product.

Note: Make sure that the client computers fulfill the uninstallation prerequisites before you attempt to uninstall Symantec Endpoint Encryption Client. See "About uninstalling the Symantec Endpoint Encryption client" on page 121.

To uninstall the Symantec Endpoint Encryption Client installation package using GPOs

1. In the navigation pane of the Management Console, expand the **Group Policy Management** snap-in.
2. Expand the domain in which you want to uninstall the client software.
3. Expand **Group Policy Objects**.
4. Right-click the GPO that you used to deploy the client software, and select **Edit**.
5. In the **Group Policy Management Editor** window, expand **Computer Configuration**.
6. Expand **Policies > Software Settings**
7. Right-click **Software installation**, and select **Properties**.
8. In the **Software installation Properties** dialog box, click the **Advanced** tab.
9. To configure the GPO to uninstall the unmanaged software packages from the subscribed computers, check **Uninstall the applications when they fall out of the scope of management**.
10. Click **OK** to close the dialog box.

11 In the navigation pane of the **Group Policy Management Editor** window, click **Software installation**.

The right pane of the window displays a list of the software packages that were deployed using this GPO.

12 Right-click the software package that you want to uninstall from all of the computers in the domain, and select **Remove**.

13 In the **Remove Software** dialog box, check **Immediately uninstall the software from users and computers** and click **OK**.

14 Close the **Group Policy Management Editor** window.

Deploying uninstallation scripts using Group Policy Objects

Deploying an uninstallation script enables you to uninstall specific Symantec Endpoint Encryption features from the client computers. Alternatively, you can also use an uninstallation script to completely uninstall Symantec Endpoint Encryption from the client computers.

Note: You can use this uninstallation method only if you used a GPO to upgrade to Symantec Endpoint Encryption 11.2.0 from an earlier product.

Before you begin

Make sure that the client computers fulfill the uninstallation prerequisites before you attempt to uninstall Symantec Endpoint Encryption Client.

See "About uninstalling the Symantec Endpoint Encryption client" on page 121.

Creating an uninstallation script file

Create a script file that includes one or more of the following commands:

- To uninstall the Drive Encryption feature:

```
MSIEXEC /i "[path]\msifile" REMOVE=DE /l*v "[logpath]\logfile"
```

- To uninstall the Symantec Endpoint Encryption for BitLocker feature:

```
MSIEXEC /i "[path]\msifile" REMOVE=BL /l*v "[logpath]\logfile"
```

- To uninstall the Removable Media Encryption feature:

```
MSIEXEC /i "[path]\msifile" REMOVE=RME /l*v "[logpath]\logfile"
```

- To uninstall the all of the Symantec Endpoint Encryption features together:

```
MSIEXEC /x "[path]\msifile" /l*v "[logpath]\logfile"
```

Where `[path]\msifile` represents the share path and name of the MSI file, and `[logpath]\logfile` represents the path and name of the output log file.

Configuring GPOs to deploy the uninstallation script

Note: If your network includes both 32-bit and 64-bit systems, make sure that you update all of the relevant GPOs.

To configure GPOs to deploy the uninstallation script

1. Open **Symantec Endpoint Encryption Management Console**.
2. In the left pane, expand **Group Policy Management** and navigate to the GPO that you previously used to upgrade the Symantec Endpoint Encryption clients..
3. Right-click the GPO and click **Edit**.
4. In the left pane of the **Group Policy Management Editor**, navigate to **Computer Configuration > Policies > Windows settings > Scripts (Startup/Shutdown)**.
5. In the right pane, double-click **Startup**.
6. On the **Scripts** tab of the **Startup Properties** dialog box, click **Add**.
7. In the **Add a script** dialog box, click **Browse**.
8. Using the navigation windows to select the uninstallation file, and then click **Open**.
9. To submit the script file, click **OK**.
10. In the **Startup Properties** dialog box, select the upgrade script that you previously used to upgrade the Symantec Endpoint Encryption clients, and click **Remove**.
11. To close the **Startup Properties** dialog box, click **OK**.
12. Close the **Group Policy Management Editor**.

Deploying the uninstallation script

After you finish configuring the GPO, restart the client computers to begin the uninstallation.

Uninstalling the Symantec Endpoint Encryption client software using the Control Panel

You can uninstall the Symantec Endpoint Encryption client software from a Microsoft Windows computer by using the Windows **Add/Remove Programs** utility. However, if the client software was installed using a Group Policy Object, it can only be uninstalled through that same GPO.

Perform the following procedure to uninstall the Symantec Endpoint Encryption client software using the **Add/Remove Programs** utility in the Control Panel.

Note: This uninstallation method removes all of the Symantec Endpoint Encryption features from client computers.

To uninstall the Symantec Endpoint Encryption client software manually:

1. Log on to the client computer using an administrator account or another account with sufficient privileges to uninstall software.
2. To access the Control Panel, do one of the following:
   - For Microsoft Windows 7, click **Start > Control Panel**.
   - For Microsoft Windows 8.x, access the **Start** screen, and type **Control Panel**. In the **Apps** search results, click the **Control Panel** icon.
   - For Microsoft Windows 10, in the **Search the web and Windows** search bar, type **Control Panel.** In the search results menu, click the **Control Panel** icon.
3. Do one of the following:
   - In the **Category** view of the Control Panel, under **Programs**, click **Uninstall a program**.
   - Click **Programs and Features**.
4. In the **Programs and Features** window, select **Symantec Endpoint Encryption Client**.
5. Click **Uninstall**.
6. If prompted to confirm, click **Yes**.
7. (Optional) If **Symantec Endpoint Encryption Autologon Client** and **Windows Password Reset Utility** are also listed in the **Programs and Features** window, uninstall them the same way.
8. After all of the clients are uninstalled, restart the computer when prompted.

Uninstalling the Symantec Endpoint Encryption client software using the command line

Client Administrators can use the command prompt to uninstall one or more Symantec Endpoint Encryption features from a single computer. You can also uninstall the Autologon Utility. The results of the uninstallation are saved in a log file that you specify.

Note: Make sure that the client computers fulfill the uninstallation prerequisites before you attempt to uninstall Symantec Endpoint Encryption Client. See "About uninstalling the Symantec Endpoint Encryption client" on page 121.

If you are prompted to restart the computer after uninstalling one or more client software, accept the prompt. When Microsoft Windows starts, return to the command prompt and enter the remaining commands to uninstall the remaining software.

Note: To perform a silent installation, append the commands in the following procedure with the `CONDITION_NOUI=1` parameter.

To uninstall Symantec Endpoint Encryption client software using the command line:

1. Click **Start > Run**.
2. In the **Run** dialog box, type cmd.
3. To open the command prompt, click **OK**.
4. (Optional) To uninstall the Autologon Utility when the Autologon feature is enabled permanently, enter one of the following commands:
   - For 32-bit systems:
     ```
     msiexec -x "[Path]\Autologon Infinite DD MMM YYYY.msi" /qn /live
     LogFilePath
     ```
   - For 64-bit systems:
     ```
     msiexec -x "[Path]\Autologon Infinite_x64 DD MMM YYYY.msi" /qn /live
     LogFilePath
     ```
5. (Optional) To uninstall the Autologon Utility when the Autologon feature is enabled by a client administrator, enter one of the following commands:
   - For 32-bit systems:
     ```
     msiexec -x "[Path]\Autologon NoAutologon.msi" /qn /live LogFilePath
     ```
   - For 64-bit systems:
     ```
     msiexec -x "[Path]\Autologon NoAutologon_x64.msi" /qn /live LogFilePath
     ```
6. (Optional) To uninstall the Drive Encryption feature, enter one the following commands:
   - For 32-bit systems:
     ```
     msiexec -i "[Path]\SEE Client.msi" REMOVE=DE /l*v LogFilePath
     ```
   - For 64-bit systems:
     ```
     msiexec -i "[Path]\SEE Client x64.msi" REMOVE=DE /l*v LogFilePath
     ```
7. (Optional) To uninstall the Removable Media Encryption feature, enter one the following commands:
   - For 32-bit systems:
     ```
     msiexec -i "[Path]\SEE Client.msi" REMOVE=RME /l*v LogFilePath
     ```
   - For 64-bit systems:

```
msiexec -i "[Path]\SEE Client x64.msi" REMOVE=RME /l*v LogFilePath
```

8 (Optional) To uninstall the Symantec Endpoint Encryption for BitLocker feature, enter one the following commands:

- For 32-bit systems:

  ```
  msiexec -i "[Path]\SEE Client.msi" REMOVE=BL /l*v LogFilePath
  ```

- For 64-bit systems:

  ```
  msiexec -i "[Path]\SEE Client x64.msi" REMOVE=BL /l*v LogFilePath
  ```

9 (Optional) To uninstall the all of the Symantec Endpoint Encryption Client features, enter one the following commands:

- For 32-bit systems:

  ```
  msiexec -x "[Path]\SEE Client.msi" /l*v LogFilePath
  ```

- For 64-bit systems:

  ```
  msiexec -x "[Path]\SEE Client x64.msi" /l*v LogFilePath
  ```

Uninstalling Symantec Endpoint Encryption for FileVault

Perform the following procedure to uninstall Symantec Endpoint Encryption for FileVault from a Macintosh computer. You do not have to decrypt the disk before uninstalling Symantec Endpoint Encryption for FileVault.

Note: Make sure that you have administrator privileges.

To uninstall Symantec Endpoint Encryption for FileVault

1 Launch the Terminal application.

2 Using Terminal, navigate to the `/Library/Application Support/Symantec Endpoint Encryption/` directory.

3 Type the following command:

```
sudo ./uninstall
```

Index

R

S

T

U

W