Symantec Endpoint Encryption Installation Guide Version 11.3.1

Table of Contents

Prerequisites for InstallingSymantec Endpoint Encryption

Symantec Endpoint Encryption system requirements

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

Table 1: Symantec Endpoint Encryption system requirements

System requirements	Article URL
Symantec Endpoint Encryption Management Server system requirements	System Requirements for Symantec Endpoint Encryption 11.3.x Management Server **Note:** Support for TLS 1.2 requires changes to the SQLDB driver. The SQLOLEDB operating system has changed to MSOLEDBSQL. This change affects the supported operating systems and SQL servers. Be sure to verify these new system requirements.
Symantec Endpoint Encryption Management Console system requirements	System Requirements for Symantec Endpoint Encryption 11.3.x Management Console
Symantec Endpoint Encryption Client system requirements	System Requirements for Symantec Endpoint Encryption 11.3.x Client

Symantec Endpoint Encryption protocols and ports

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

Table 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.
Lightweight Directory Access Protocol (LDAP)	TCP/IP	Query Active Directory and eDirectory directories	Symantec Endpoint Encryption Management Server	389, 3268, or configurable

Application layer protocol	Communication protocol	Purpose	Used by	Port
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

About configuring TLS/SSL communications for Symantec Endpoint Encryption

Accounts required by Symantec Endpoint Encryption

Symantec Endpoint Encryption requires the following accounts:

Table 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`
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. Setting up the rights for the database access account
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.
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.

Accounts required by Symantec Endpoint Encryption

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 11.3.1, 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

Element	Access
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:
- 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 11.3.1 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 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.

Changing the Management Password

Symantec Endpoint Encryption Microsoft SQL Server software download requirements

The SQL Server requires the two following downloads:

- The Microsoft SQL Server Feature Pack
- The MSOLEDBSQL driver

For the Feature Pack, download the following software from the specified URL:

- Microsoft System CLR Types for SQL Server 2012 (32-bit)
- Microsoft SQL Server 2012 (32-bit) Management Objects

NOTE

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

https://www.microsoft.com/en-us/download/details.aspx?id=56041

For the MSOLEDBSQL driver, download the driver from this URL:

https://docs.microsoft.com/en-us/sql/connect/oledb/download-oledb-driver-for-sql-server?view=sql-server-ver15

Enabling and installing prerequisites for the Management Console

When you install the Symantec Endpoint Encryption Management Console, the prerequisites and installation steps differ, based on whether you are installing the Management Console on a Windows server or a Windows client.

- For installing the Management Console on a Windows server operating system
  - Install all of the Symantec Endpoint Encryption Management Server prerequisites, following the procedure for your Windows server class system.
    Windows server installations: Enabling roles, features, and tools for the Symantec Endpoint Encryption Management Server
  - Install the Management Console using a custom install.
    Installing a Management Console
- For installing the Management Console on a Windows client operating system
  - Install the Remote Server Administration Tools.
    Windows client installations: Installing Remote Server Administration Tools for the Management Console
  - Install the Management Console using a custom install.
    Installing a Management Console

Windows server installations: Enabling roles, features, and tools for the Symantec Endpoint Encryption Management Server

The procedure below enables the prerequisite server roles, features, and tools to install Symantec Endpoint Encryption. Completing this procedure is required to install the product, including the Management Console.

Before installing the Management Console on a server class system (Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019), follow the procedure for your server class system. The procedure includes the installation of the Remote Server Administration Tools and the .NET framework. You must also separately download the Microsoft SQL Server Feature Pack as well as the MSOLEDBSQL driver.

Symantec Endpoint Encryption Microsoft SQL Server software download requirements

On Microsoft Windows Server 2019

To enable the Web service (IIS) role on a Microsoft Windows 2019 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 4.7 Features** and check **.NET Framework 4.7** and **ASP.NET 4.7**.
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 4.7**
    - **ASP .NET 4.7**
    - **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 2016

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

20. Go to **Start > Programs > Administrative Tools > Server Manager**.
21. In the **Dashboard**, click **Add roles and features**.
22. In the **Add Roles and Features Wizard**, click **Next**.
23. In the **Installation Type** page, click **Role-based or feature-based installation** and then click **Next**.
24. In the **Server Selection** page, make the selection that matches your environment and then choose your server and click **Next**.
25. In the **Server Roles** page, select **Web Server (IIS)**.
26. In the **Add Roles and Features Wizard** window, click **Include management tools** and then click **Add Features**.
27. Click **Next**.
28. In the **Features** page, expand **.NET Framework 4.6 Features** and check **.NET Framework 4.6** and **ASP.NET 4.6**.
29. In the **Features** page, check **Group Policy Management**.
30. In the **Features** page, expand **Remote Server Administration Tools > Role Administration Tools** and check **AD DS and AD LDS Tools**.
31. Click **Next**.
32. In the **Web Server Role (IIS)** page, click **Next**.
33. In the **Role Services** page, expand **Web Server > Security** and select **Basic Authentication** and **Windows Authentication**.
34. 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**
35. 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**
36. Click **Next**.
37. In the **Confirmation** page, click **Install**.
38. In the **Results page**, click **Close**.

On Microsoft Windows Server 2012

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

39. Go to **Start > Programs > Administrative Tools > Server Manager**.
40. In the **Dashboard**, click **Add roles and features**.
41. In the **Add Roles and Features Wizard**, click **Next**.
42. In the **Installation Type** page, click **Role-based or feature-based installation** and then click **Next**.
43. In the **Server Selection** page, make the selection that matches your environment and then choose your server and click **Next**.
44. In the **Server Roles** page, select **Web Server (IIS)**.
45. In the **Add Roles and Features Wizard** window, click **Include management tools** and then click **Add Features**.
46. Click **Next**.
47. In the **Features** page, expand **.NET Framework 4.5 Features** and check **.NET Framework 4.5** and **ASP.NET 4.5**.
48. In the **Features** page, check **Group Policy Management**.
49. In the **Features** page, expand **Remote Server Administration Tools > Role Administration Tools** and check **AD DS and AD LDS Tools**.
50. Click **Next**.
51. In the **Web Server Role (IIS)** page, click **Next**.
52. In the **Role Services** page, expand **Web Server > Security** and select **Basic Authentication** and **Windows Authentication**.
53. 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**
54. 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**
55. Click **Next**.
56. In the **Confirmation** page, click **Install**.
57. In the **Results page**, click **Close**.

Windows client installations: Installing Remote Server Administration Tools for the Management Console

Before installing the Management Console on a client running Windows 8 or 10, you must install:

- The .NET framework
- The MSOLEDBSQL driver
  Microsoft SQL Server software download requirements
- The Remote Server Administration Tools

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 10

1. Download and install the Microsoft Remote Server Administration Tools for Microsoft Windows 10 from:
   https://www.microsoft.com/en-us/download/details.aspx?id=45520

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

2. 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

Installing and Upgrading the server

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.

About using TLS 1.2

As of version 11.3.0, Symantec Endpoint Encryption uses TLS 1.2 as the default communication protocol. During installation, TLS 1.0 and TLS 1.1 are disabled. During an upgrade, if TLS 1.0 or TLS 1.1 were enabled, they remain enabled. After an installation or upgrade, go to the Configuration Manager and use the **Disable TLS 1.0 and TLS 1.1** option on the Web Server Configuration page to enable or disable these previous protocol versions. Enable the previous protocol versions for backward compatibility if:

- You have clients earlier than Symantec Endpoint Encryption 11.1.0, including Symantec Endpoint Encryption 8.2.1 clients, reporting to the Symantec Endpoint Encryption Management Server. These clients use TLS 1.0.
- You have Mac clients with FileVault 2 running previous versions of Symantec Endpoint Encryption, which used TLS 1.0; otherwise, Mac clients with FileVault 2 enabled can connect to the Symantec Endpoint Encryption Management Server using only TLS 1.2.

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 the Server

To install your Symantec Endpoint Encryption Management Server, complete the following tasks:

Table 4: Process for Installing 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. **Note:** TLS 1.2 has a different set of supported operating systems and SQL servers; be sure to double-check the 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. Symantec Endpoint Encryption Microsoft SQL Server software download requirements
Meet the prerequisite services requirements	Verify that IIS is installed and enable the web server (IIS) server role and the required role services. Windows server installations: Enabling roles, features, and tools for the Symantec Endpoint Encryption Management Server
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. About configuring TLS/SSL communications for Symantec Endpoint Encryption
Run the installation wizard	Run the installation wizard to specify your settings for the server. When you install the Symantec Endpoint Encryption Management Server, you specify the initial settings for the Symantec Endpoint Encryption database and its communications. You can later change these settings in the **Configuration Manager** utility if you need to. Installing the server
Configure the Server	You use the configuration wizard to set up your directory service synchronization and to configure the Web service. Configuring the server
Restart the server	After you finish the steps, restart the computer.
Complete the installation	After finishing the installation wizard and the configuration wizard, verify that you installed the server correctly and then back up the database. Completing the installation

Installing the server

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

To install 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 with which you are going 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.

NOTE
Beginning with the Symantec Endpoint Encryption 11.3.1 release, there is no separate MSI file for Autologon. Therefore, when you upgrade the Symantec Endpoint Encryption Management Server to 11.3.1 and later, you can optionally uninstall the existing Autologon MSI from the Symantec Endpoint Encryption Management Server.

5. On the **Welcome** page of the wizard, click **Next**.
6. In the **License agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. 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**.
   - To enable specific features, click **Custom** and then 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**.

Destination folder	Lets you change where Symantec Endpoint Encryption stores its program files. Select the feature you want to change and then click destination folder. Browse to the location where you want to store the files and then click **OK**.

8. On the **Custom Setup** page, click **Next**.
9. On the **Database Location and Credentials** page, in the **Database Instance** field, provide the location of the database. 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`.

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

    To use this feature, you must meet additional prerequisites.

    About configuring TLS/SSL communications for Symantec Endpoint Encryption
11. If your database server is configured to use a custom port, select **Custom port number** and enter the port number.
12. 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.

    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. If you select **SQL authentication**, the **Web Application Identity** field appears. You can change the identity from being the default Network Service account to a custom account. A custom account is the AD credential of a domain user. Supplying a custom account lets the web-based Help Desk Recovery console access Active Directory for the user's User Group association. Best practices for Microsoft SQL Server database logons

13. Click **Next**.
14. On the **Database Access** page, do one of the following:
    - Click **Create a new database**. You can either accept the default database name or enter a custom name.
    - If you want to use an existing database, click **Use existing database**.

15. Click **Next**.
16. On the **Database Access** page, do one of the following according to your authentication method:

Windows authentication	Specify the Microsoft Windows account on the Symantec Endpoint Encryption Management Server. This account has the following characteristics: • It is a service account for the Services website. • It is a logon account for the synchronization services. • It has membership in the `IIS_WPG` group. • Log on as a service In the **User name** field, enter the user name and password account name in NetBIOS format. After you specify the account, the installer validates it. A message is displayed indicating that it exists. If the account is valid, click **Yes**. 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**.
SQL authentication	Choose if you want to create a new login or to use an existing login. When creating a new database, you can either specify a new SQL account or use an existing SQL account. When using an existing database, you must use an existing SQL account. • To create a new SQL account, click **Create a new login**. Enter the user name, password, and the password confirmation of the new account. • To use an existing SQL account, click **Use existing login**. Enter the credentials of the database communications account that you created during your previous installation. Use the following for setting up SQL Server database logins: Best practices for Microsoft SQL Server database logons Setting up the rights for the database access account

17. Click **Next**.
18. In the **Database Configuration** page, you can specify custom configuration settings. Accept the default configuration settings. You can change your database configuration settings later by using the Microsoft SQL Server tool of your choice. Do not use the Symantec Endpoint Encryption Configuration Manager for this purpose. It only lets you increase the size settings but not decrease them. If you change paths it requires you to detach and reattach the Symantec Endpoint Encryption database.

    Do one of the following:

    - Accept the default database configuration.
      Leave the **Customize my database configuration** check box deselected.
    - Select **Customize my database configuration** then do the following:
      – Enter the paths for the data file and the log file. The directories in this path must already exist on the database server. The installer does not create the directories.
      – Enter the file size values in megabytes for the data and log files. These sizes include autogrowth size, initial size, and maximum size. Make sure that the database server has enough space for the data and log files.

19. Click **Next**.
20. On the **SEE Management Password** page, do the following:

    - In the **SEE Management Password** dialog box and the **Confirm Password** dialog box, provide the Symantec Endpoint Encryption Management Password.

      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.

21. Click **Next**.
22. On the **Ready to Install the Program** page, click **Install**.
23. On the **Installation Wizard Completed** page, click **Finish**.

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

    Configuring the server

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.

NOTE

If you will be using Kerberos authentication for the web-based Help Desk Recovery console, you configure those settings also using the configuration manager. However, before you implement Kerberos, you must complete prerequisite tasks. Preparing the environment for Kerberos authentication

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. About configuring TLS/SSL communications for Symantec Endpoint Encryption
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.

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.

    About configuring TLS/SSL communications for Symantec Endpoint Encryption
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. Click **Next**.
22. On the **Directory Synchronization** page, to synchronize your directory service, click **Activate Directory Synchronization**.
23. 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**.

24. Click **Finish**.
25. Click **Restart** if prompted.

Preparing the environment for Kerberos authentication

About Kerberos authentication

Kerberos is a network authentication protocol that uses tickets to allow nodes communicating over a non-secure network to prove their identity to one another securely. For a help-desk administrator authenticating from their client browser to the Symantec Endpoint Encryption web-based Help Desk Recovery console, using Kerberos means using a single-click login, rather than a form-based (user/password) login.

Configuring Kerberos authentication

To enable Kerberos authentication, you must configure multiple settings using two interfaces:

- The Symantec Endpoint Encryption Management Server Configuration Manager

  NOTE

  Even though you can set some of the server and database fields in the Symantec Endpoint Encryption Suite Installation Wizard, to access all configuration pages necessary for Kerberos, after Symantec Endpoint Encryption is installed, launch the Configuration Manager program.
- The MS Windows elevated command line

Table 5: Process for enabling Kerberos authentication for web-based Help Desk Recovery console

Step/Task	Interface	Page or command	Field	Note
1. Define the mode in which Symantec Endpoint Encryption Management Server authenticates to the database.	Config Mgr	Database Configuration	**Authentication mode**: **Windows authentication** OR **SQL Server authentication / Web application pool identity**	For **Windows authentication**: Define a Windows domain account. If the deployment uses multiple servers with a load balancer, use the same account across all servers. For **SQL Server authentication**: **Note:** Selecting **SQL Server authentication** causes the **Web application pool identity** field to appear. For the **Web application pool identity** field • If you are using a single server, let the field default to your Network Service account. • If you are using multiple servers with a load balancer, change the field to a Windows domain account. Use the same account across all servers.
2. If you defined the **Web application pool identity** to be a Windows domain account, the AD administrator must run two “set” commands on Symantec Endpoint Encryption Management Server. **Note:** Commands require Domain Admin privileges.	CLI	`setspn`		Configure the Service Principal Name (SPN) to the server resource name. Running the "set" commands for Kerberos authentication
		`set-ADUser`		Set the AD Windows domain user to have trusted delegation to run the Kerberos service. Running the "set" commands for Kerberos authentication

Step/Task	Interface	Page or command	Field	Note
3a. Set client communications to use Windows authentication.	Config Mgr	Web Server Configuration	**Enable Windows Authentication**	Select this field for client communication, to use more secure Windows Authentication. If disabled, client communication fallback is to Basic Authentication. **Note:** Selecting this field causes the **Custom SPN configuration** field to appear.
3b. Indicate in the Configuration Manager that the "setspn" command has been executed.		Web Server Configuration	**Custom SPN configuration**	Select this checkbox to indicate that the Service Principal Name has been customized, changing the website settings. After you save this website configuration, you must reset IIS.
4. Choose Kerberos to be the authentication method for the web-based Help Desk Recovery console.	Config Mgr	Help Desk Configuration	**One-Click Login Authentication**	To have form-based authentication as a backup or alternative to Kerberos, choose **Both (Form based and One-Click Login)**. See the Configuration Manager online help for a description of the Help Desk page.
5. Configure the supported client browsers to enable Kerberos authentication.	CLI or GPO			Configuring endpoint browser settings for Kerberos authentication

Running the "set" commands for Kerberos authentication

Two commands are required for Kerberos authentication, if you are running with multiple servers using a load balancer, and:

- You chose **Windows authentication** on the Database Access page in the Symantec Endpoint Encryption Installation Wizard or the Database Configuration page in the Configuration Manager and defined a Windows domain account, or
- You chose **SQL Server authentication** and defined a Windows domain account for the **Web application pool identity**.

NOTE

These commands are not required when **SQL Server authentication** is selected for a single Symantec Endpoint Encryption Management Server installation, since the local system Network Service account authenticates in-bound Kerberos tickets.

NOTE

Running these commands requires Domain Admin privileges.

To associate the Web application pool identity for Kerberos authentication delegation

1. On the Symantec Endpoint Encryption Management Server, from an elevated command prompt, enter:

   ```
   setspn -s HTTP/<{{SEEMgmtServer}}> <Domain>\<KerberosUser>
   ```

   Where <KerberosUser> is the Windows account name.

   The SPN (Service Principal Name) command associates the **Web application pool identity** with the server resource name.

2. From an elevated Windows PowerShell, enter:

   ```
   Set-ADUser <KerberosUser> -TrustedForDelegation 1
   ```

   The command modifies an instance of the ADobject and updates Active Directory, allowing the Kerberos user to have trusted delegation for Kerberos authentication.

Configuring endpoint browser settings for Kerberos authentication

To enable One-Click Login (Kerberos authentication) for the web-based Help Desk Recovery console, you must modify the following browser settings as shown in Endpoint browser settings for Kerberos authentication.

Table 6: Endpoint browser settings for Kerberos authentication

OS: Browser	Manual setting	Enterprise deployment
Windows: • Internet Explorere • Edge • Google Chrome	Add a manual setting to keep the <Symantec Endpoint Encryption Management Server/Load Balancer URL> in the Local Intranet Zone.	You can use a GPO to configure Site Security Zone mappings. To edit the GPO, in the Active Directory snap-in: 1. Navigate to **User Settings > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page**. 2. Enable the "Site to Zone Assignment List" policy. 3. Set **Value Name** to "<Symantec Endpoint Encryption Management Server/ Load balancer URL>" and **Value** to **1** (1 = Local Intranet).
Mac: • Safari	No manual settings are required.	This browser works as is, once the endpoint computer is in the domain.
Windows, Mac: • Mozilla Firefox	1. Navigate to `about:config`. 2. Search for “network.negotiate-auth.trusted-uris”. 3. Set the value to “<Symantec Endpoint Encryption Management Server/Load balancer URL>”.	Firefox has GPO policy configuration options to manage these settings. Click this link for instructions: https://support.mozilla.org/en-US/kb/customizing-firefox-using-group-policy-windows Once you set up the ADMX files, edit the GPO by configuring the <Symantec Endpoint Encryption Management Server/Load balancer URL> at **User Settings > Administrative Templates > Mozilla > Firefox > Authentication > SPNEGO**.

Installing 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 Install a Management Console:

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

   Accounts required by Symantec Endpoint Encryption

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 **License agreement** page, select **I accept the terms in the license agreement** and click **Next**.
7. On the **Setup Type** page, to install Management Agent, select **Custom**.
8. 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**.
Destination folder	Lets you change where Symantec Endpoint Encryption stores its program files. Select the feature you want to change and then click destination folder. Browse to the location where you want to store the files and then click **OK**.

9. 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**.

10. In the **Database Server** page, click **Use SEE Server** to install the Management Console with the default settings.
11. 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.
12. 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.
13. Click **Enable TLS/SSL** if you configured your database to use TLS/SSL encryption.

    About configuring TLS/SSL communications for Symantec Endpoint Encryption
14. 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**.
15. 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.

    Accounts required by Symantec Endpoint Encryption
16. Click **Next**.

    The installation wizard authenticates to the database server that you specified, and it verifies that the account credentials are correct.
17. 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.
18. Click **Next**.
19. In the **Ready to Install the Program** page, click **Install**.
20. 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**.

Installing 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 install 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 installation

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:

7. Access the Symantec Endpoint Encryption database with the Microsoft SQL Server Management Studio.
8. 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.

Creating installers for the Symantec Endpoint Encryption clients

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 Mac 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 Mac computers. The compressed folder consists of the SEEInstaller.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 11.3.1 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 client installation package identifies the client computers to the Symantec Endpoint Encryption Management Server for tracking and reporting purposes and for computer access recovery.

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 package is created and saved in a zip archive. The SEEInstaller.zip folder consists of the SEEInstaller.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 or macOS package.
  The individual settings that you selected for a given feature are saved in a date- and time-stamped log file.
  For an MSI, the log file is “ManagementAgentSettings <date&time>.log"
  For macOS package, the log file is "MacClientSettings <date&time>.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.

About enabling features in the Symantec Endpoint Encryption Client installation package

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 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 Login Attempts section:
  - The **Limit Login 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

4. 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.
   - Select a policy group from the **Preferred Policy Group** dropdown list that you want to assign to client computers at install-time. When you select a preferred group name from the dropdown list, its respective Fully-Qualified Domain Name (FQDN) path along with group name is displayed on the screen.
     By default, clients are assigned to the SEE Unassigned group.
5. Click **Next**.

   Management Agent Installation Settings – Advanced Settings page

   NOTE

   The Advanced Settings are not applicable to FileVault.
6. On the **Management Agent Installation Settings – Advanced Settings** page, do the following:
   - Click **Edit**. All fields become available for update.
     Click **Restore defaults** at any time before you click **Next** to reset fields to their default values.
   - To define an AD User Group for which client administrator rights are granted to members, in the **Value** column for the setting **Client Admin Privilege (AD User Group)**, enter an AD User Group. Use the syntax: DOMAIN\NAME. If you do not want to define a group, leave the field empty. Previously, the setting name was de.clientAdmin.adGroupName.
     The default value is blank.
   - To allow a user running a SYSTEM user account to execute Autologon commands without client administrator credentials, in the **Value** column for the setting **Allow Autologon Management for SYSTEM User**, enter **True**. To disable this feature, enter **False**. Previously, the setting name was de.autoLogon.allowSystemUserManagement.
     The default value is **False**.
   - Using TPM and PCR configurations, the computer environment can be hardened by disabling Autologon if changes occur in a computer's hardware/platform environment. To define the active TPM Platform Configuration Registers (PCRs) when Autologon is enabled, in the **Value** column for the setting **Platform Config Registers (PCR) Values**, enter the desired PCR numbers, separated by commas. Allowed numbers are 0, 1, 2, 3, 4, or any combination thereof. Previously, the setting name was de.autoLogon.pcrList.
     The default values are **0,2**.
     Caution: Aggressive settings may result in frequent and unintended Autologon failures. See especially the policy configuration topic referenced in Step 2, for a more extended discussion of the settings.
   - You can enable automatic shutdown at the UEFI preboot screen on the client systems. This automatically shuts down the client system if there is no user activity on the UEFI preboot screen for the specified timeout interval.
     To define the idle timeout after which the system automatically shuts down in the **Value** column for the setting **Preboot Auto Shutdown Timeout**, enter the timeout interval in minutes. Previously, the setting name was de.preboot.autoShutdownTimeout.
     The default value is **0**. This value disables automatic shutdown.
     The minimum idle timeout value is 5 minutes.
   - You can enable single sign-on for users when they resume from hibernation on a client computer. After hibernation, the users are automatically logged on to Windows after the users authenticate with Windows credentials at preboot.
     To enable single sign-on on a client computer when resumed from hibernation, in the **Value** column for the setting **Allow SSO with Hibernation**, enter **True**. Previously, the setting name was de.sso.allowWithHibernation.

To disable this feature, type **False**. This setting is disabled by default.

- To define an Active Directory user group whose members can uninstall a standalone Symantec Endpoint Encryption client from end-user systems, in the **Value** column for the setting **Allow Client Uninstallation (AD User Group)**, enter an Active Directory User Group name. Use the syntax: DOMAIN\NAME. If you do not want to define a group, leave the value empty. Previously, the setting name was ma.uninstall.adGroupName.
  The default value is blank.

  NOTE
  The **Allow Client Uninstallation (AD User Group)** advanced setting is applicable to BitLocker or Removable Media Encryption (RME) installers. However, it is not applicable to FileVault installers.
- To allow only the SYSTEM user to uninstall the Symantec Endpoint Encryption client, type **True** in the **Value** column corresponding to the **Allow Client Uninstallation for SYSTEM User only** Advanced Settings option. This setting prevents local users from uninstalling the Symantec Endpoint Encryption client. This setting is disabled by default.
- If users experience file corruption issues while burning files using the Symantec Removable Media Encryption Burner Application, then ttype **True** in the **Value** column corresponding to the **Enable Alternate File Writing Method for CD/DVD Burner** Advanced Setting option to resolve the issue. This setting is disabled by default.

7. Click **Next.**

   For more information about Advanced Settings, see "Configuring the Management Agent - Advanced Settings policy options" in the *Symantec Endpoint Encryption Policy Administrator Guide*.

8. Do one of the following:

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

   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.

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
4. 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**.
5. 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.
6. Click **Next**.

   Drive Encryption Installation Settings – Single Sign-On page

7. 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.
8. Click **Next**.

Drive Encryption Installation Settings – Self-Recovery page

9. 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.
10. 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

11. 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.

12. 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.
13. 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.
14. Click **Next**.

    Drive Encryption Installation Settings – Logon History page
15. 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.
16. Click **Next**.

    Drive Encryption Installation Settings – Autologon page

    About Autologon
17. On the **Drive Encryption Installation Settings - Autologon** page, do the following:
    - In the **Autologon** section, select the **Do not use Autologon** policy option to disable autologon completely. In this case, you cannot enable autologon on the client computers even through Drive Encryption Administrator Command Line or using policies. To enable autologon in such a case, you need to uninstall the client and install again with the **Do not use Autologon** policy option deselected.
      If you deselect the **Do not use Autologon** policy option at install-time, only then you can create and apply an install-time, GPO, or native policy to enable or disable the various autologon policy settings on a client computer. These various Autologon policy settings are:
      - Autologon Settings
      - Autologon Precedence settings
      - TPM settings
    - In the **Autologon Settings** section, do one of the following:
      - To disable autologon on a client computer, click the **Never Autologon** policy option. Assign this policy to one or more client computers on which the autologon is already enabled. Applying this policy on a computer disables

autologon. When a user starts the client computer on which this policy is applied, the computer prompts for user authentication at preboot. The client computer boots into Windows only after successful user authentication.

- To enable a client administrator to use the Administrator Command Line and manage autologon, click the **Autologon only when activated by admin locally** policy option.
- To enable autologon on a client computer, click the **Always Autologon** policy option. Assign this policy to one or more client computers to enable autologon. When a user starts a client computer on which this policy is applied, the client computer boots Windows without prompting for user authentication. This setting provides little protection to client computers. This option is selected by default.

- In the **Autologon Precedence** section, 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**.
- In the **TPM Settings** section, to enable Trusted Platform Module (TPM)-based authentication for Autologon users, under TPM Settings, check **Use TPM if available**.

  NOTE

  - 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.

18. Click **Next**.

Drive Encryption Installation Settings – Encryption page

NOTE

Beginning with Symantec Endpoint Encryption 11.2.1, you can enable or disable automatic encryption on client computers. You can enable automatic encryption by specifying disks as well as their partitions using the install-time policy options.

19. 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 **Enable automatic encryption** to automatically encrypt the selected disks and their specific partitions after installation of the Symantec Endpoint Encryption client.
  - Select **Boot disk** or **All disks** to specify which disks you want to encrypt.
  - Select **Boot partition, All partitions,** or **Partition list** to specify which partitions you want to encrypt for the selected disk.

    NOTE

    If you select the **All disks** option, then the **Boot partition** option is disabled.

    Hardware encryption for Opal v2 compliant drives is supported only on the entire disk and not on individual partitions. To use hardware encryption, choose the **All disks** and **All partitions** options. If

you select the **Boot partition** or **Partition list** option with hardware encryption policy enabled, then auto-encryption does not start on the Opal v2 compliant drives.

- 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.

20. Click **Next**.

    Drive Encryption Installation Settings – Client Monitor page

21. 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.

22. Click **Next**.

    Drive Encryption Installation Settings – Help Desk Recovery page

23. 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.

24. Click **Next**.

    Drive Encryption Installation Settings – Self-Encrypting Drives page

25. 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: https://support.symantec.com/en_US/article.TECH251592.html.

    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.

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

    Configuring the Removable Media Encryption installation settings

    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 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, and you may select an encryption mode. For all Windows systems, the AES encryption strength of 256-bit is enabled by default. For the encryption mode, the **Prefer the XTS-AES encryption mode, if available** check box is enabled by default.

      NOTE

      - The changes in the encryption policy option have no effect if the volumes are already encrypted or if encryption is in progress.
      - The change in the encryption strength is effective for the volumes that are not encrypted.
      - The XTS-AES encryption mode is supported only on Windows 10 version 1511 and later. However, if you have enabled the XTS-AES encryption mode on a system running a Windows 10 version that is earlier than version 1511, the encryption mode is automatically set to AES.
    - 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
6. 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.
7. If you chose to enable Removable Media Encryption, click **Next** to configure the Removable Media Encryption installation settings. Configuring the Removable Media Encryption installation settings

   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 11.3.1 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

4. 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, serial number (optional) and an optional description in the fields provided.

    Serial number can be used to exempt specific devices on Removable Media Encryption clients version 11.3 and later. Policies applied on clients with earlier versions only filter based on Vendor ID and Product ID. Serial number can contain alphanumeric characters, '&', '_'; and wildcards '?' and '*'. If unspecified, the serial number filter is equivalent to '*'.
  - To exempt all the devices from a vendor, do the following:
    - type the vendor ID in the **Vendor ID** box.
    - type the wildcard character * in the **Product ID** box
    - type an optional description in the **Description (Optional)** box

5. Click **Next**.

   Removable Media Encryption Installation Settings - Encryption Method page
6. 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.
7. Click **Next**.

   Removable Media Encryption Installation Settings - Default Passwords page
8. 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.

9. Click **Next**.

Configuring the Management Agent installation settings

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.

10. 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.

11. Click **Next**.

Removable Media Encryption Installation Settings - Portability page

12. 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.

13. Click **Next**.

Removable Media Encryption Installation Settings - Expired Certificates page

14. 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.
15. Click **Finish**.
16. In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.
17. (Optional) Change the default package name to a name of your choice.
18. 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 additional features on Microsoft Windows clients

You can create and deploy a new Symantec Endpoint Encryption Client installation package to modify the number of features that are installed on version 11.3.1 client computers. First ensure that the disk is already fully encrypted or decrypted. If disk encryption or decryption is in progress, wait until the operation is complete before you deploy the installation package.

Deploying client installers using the command line

For information about deploying the Symantec Endpoint Encryption Client installation package to install additional features on client computers, see

NOTE

You cannot use the Windows Client Installation Settings wizard to remove features from client computers. You must uninstall the unwanted features individually. About uninstalling the Symantec Endpoint Encryption client

Creating a Symantec Endpoint Encryption Client installation package

Table 7: Modifying features in the Symantec Endpoint Encryption Client installation package

Features that are already installed	Features that you want to add	Features that you must enable in the client installation package
Drive Encryption	Removable Media Encryption	• Drive Encryption • Removable Media Encryption OR Removable Media Encryption only
Removable Media Encryption	Drive Encryption	• Drive Encryption • Removable Media Encryption OR Drive Encryption only
Removable Media Encryption	Symantec Endpoint Encryption for BitLocker	• Symantec Endpoint Encryption for BitLocker • Removable Media Encryption OR Symantec Endpoint Encryption for BitLocker only
• Symantec Endpoint Encryption for BitLocker • Removable Media Encryption	Drive Encryption	This is not a valid feature combination.
• Drive Encryption • Removable Media Encryption	Symantec Endpoint Encryption for BitLocker	This is not a valid feature combination.

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.

NOTE

You can use only a native policy to update the install-time policy setting for automatic FileVault encryption and Autologon.

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 **FileVault - Introduction** page, click **Next**.
3. On the **FileVault – 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 **FileVault – Institutional Recovery Key** panel. To select a different Institutional Recovery Key certificate file, click **Change Key**.
4. Click **Next**.
5. On the **FileVault - Encryption and Autologon** page, do the following:
   - Select **Enable automatic FileVault encryption** to automatically encrypt the disks after installation of the Symantec Endpoint Encryption for FileVault client on a Mac computer.
   - Select **Enable Autologon** to enable Autologon so that the users bypass the FileVault preboot authentication screen when they log on to the Mac computer.
   - In the **User credentials for Autologon and Secure Token management** section, enter username of a pre-provisioned FileVault user account in the **Username** box. Type the password for this pre-provisoned FileVault user account in the **Password** and **Confirm Password** boxes. You need to enter this FileVault user's credentials so that the following occurs:
     – Enable or disable Autologon
     – Enable Secure Token for an user, whose Secure Token is not already enabled.
       To enable Secure Token, the pre-provisioned FileVault user needs to have administrator privileges.
6. Click **Next**.
7. On the **FileVault - 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.
8. Click **Finish**.
9. In the **Save Mac Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption for FileVault installation package.
10. If required, change the default Symantec Endpoint Encryption for FileVault package name.
11. 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 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 Autologon

NOTE
Beginning with the Symantec Endpoint Encryption 11.3.1 release, the Autologon policy options are bundled with the Drive Encryption MSI, and no separate Autologon utility is required to install on the client system.

Use Autologon to configure Microsoft Windows client computers to bypass the preboot authentication screen that the 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 Autologon is in a state of heightened vulnerability. Using Autologon 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, you should disable the Autologon function immediately after you finish updating 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.

Autologon commands can be run by two groups of users in addition to client administrators: privileged users and local SYSTEM users. Neither of these groups enters client administrator credentials, but both must authenticate to a UAC prompt and have Windows Administrator rights. Both of these groups are defined by a policy administrator on the Advanced Settings page of the Symantec Endpoint Encryption Management Agent. The policy can be deployed as an installation setting, GPO, or native policy.

- Privileged users--The policy administrator enables privileged users by specifying an AD User Group that has client administrator privileges. The user members can access the Drive Encryption Administrator Command Line and

execute Autologon commands without including client administrator credentials. (These users also have access to the Client Administrator Console and have the privileges of a default client administrator, including disk management, user management, and client-server check-ins.)

- SYSTEM users--The policy administrator can enable SYSTEM users to run Autologon commands. SYSTEM users can run only Autologon commands and do not have privileges for other Drive Encryption capabilities. The benefit is largely in allowing scripts that run remotely to be more secure, by invoking commands that enable and disable Autologon without including client administrator credentials in the clear.

NOTE

The Advanced Settings page is not applicable to FileVault, BitLocker, or Removable Media Encryption (RME) installers.

Deploying new clients

Deploying client packages using a third-party tool

Installation of the Symantec Endpoint Encryption Client packages can be accomplished using any third-party deployment tool that supports the MSI format. To avoid installation errors, make sure that when you create the client installer packages that you save them to a local hard disk or other volume which includes Full Control permissions. The client installer packages can then be copied to removable media, a network volume accessible to the client, or the local hard disk of the client computer.

NOTE

If you run the Symantec Endpoint Encryption Client installation package to modify the number of features that are installed on the client computer, first ensure that the disk is already fully encrypted or decrypted. If disk encryption or decryption is in progress, wait until the operation is complete.

Deploying new clients using Group Policy Objects

You can deploy the Symantec Endpoint Encryption Client installer using Active Directory. Use a GPO to include the MSI file, and establish a shared distribution location that client computers access. Tailor these procedures to suit the requirements of your organization.

NOTE

If you run the Symantec Endpoint Encryption Client installation package to modify the number of features that are installed on the client computer, first ensure that the disk is already fully encrypted or decrypted. If disk encryption or decryption is in progress, wait until the operation is complete.

Creating Symantec Endpoint Encryption Client installers for distribution

1. **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.

   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*.

   Creating a Symantec Endpoint Encryption Client installation package

   Creating an Active Directory distribution point

2. **To create a distribution point on your Active Directory forest or domain:** 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.

3. 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 GPOs to deploy the installer MSI

To create Group Policy Objects and deploy the client installer

NOTE

To deploy the client installer package with a GPO, you must install is as a part of a software installation computer policy and not as part of a software installation user policy. Also, ensure that you create separate GPOs for 32-bit and 64-bit packages.

NOTE

If User Account Control (UAC) is enabled on a client computer, you must enable the Always install with elevated privileges group policy setting for Computer Configuration and User Configuration before you install the client installation package with a GPO.

4. Open **Symantec Endpoint Encryption Management Console**.
5. In the left pane, expand **Group Policy Management**.
6. Right-click **Group Policy Objects** and click **New**.
7. In the **New GPO** window, type a GPO title in the **Name** box and click **OK** to save the new policy.
8. Right-click the created GPO, and select **Edit**.
9. In the **Group Policy Management Editor**, expand **Computer Configuration** and navigate to **Policies** and **Software settings**.
10. Right-click **Software Installation**, and select **New** > **Package**.
11. Navigate to the distribution point where you previously saved the Symantec Endpoint Encryption client installer.
12. Select the MSI that you want to include in a GPO for deployment and click **Open**.

NOTE

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

13. In the **Deploy Software** dialog box, accept the default value of **Assigned** and click **OK** one or more times as prompted.
14. Close the **Group Policy Management Editor**.

Installing the client installer GPOs

After the deployment is complete, to begin the software installation, restart the client computers.

Installing the client software manually

About installing the client software manually

Apart from the infrastructure-based deployment, the Symantec Endpoint Encryption client software can be manually installed on individual client computers. Manual installation is useful when the setup has only a few clients or other deployment methods are unavailable.

Preparing to install the client software manually

Before installing the client software, you must do the following:

- Ensure that you log on to the client computer with administrator privileges with sufficient rights to install software.
- For Windows clients, determine whether the client computer has a 32-bit or 64-bit version of Microsoft Windows.
- Identify the Symantec Endpoint Encryption Client installation package that is compatible with the version of Windows running on the client computer.
- Provide access to the client installation packages either through a network share or using a removable storage device.

NOTE

If you run the Symantec Endpoint Encryption Client installation package to modify the number of features that are installed on the client computer, first ensure that the disk is already fully encrypted or decrypted. If disk encryption or decryption is in progress, wait until the operation is complete.

Installing Symantec Endpoint Encryption Client

To manually install Symantec Endpoint Encryption Client

1. Double-click the SEE Windows Client.msi file or the SEE Windows Client_x64.msi file.
2. When prompted to restart, click **Yes** to restart your system and complete the installation.

Installing Symantec Endpoint Encryption for FileVault

To manually install Symantec Endpoint Encryption for FileVault

3. Double-click the `SEEInstaller` installation package file.
4. On the **Welcome to the Symantec Endpoint Encryption Installer** window, click **Continue**.
5. Read and agree to the Software license agreement and complete the installation.

NOTE

When prompted, enter the administrator user name and password to install the software.

NOTE

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) or later installed.

Installing the client with support for Windows 10 feature update through Windows updates

You can install client and leverage the support for Windows 10 feature update through Windows updates on a computer with drives that are encrypted with Symantec Endpoint Encryption by performing the steps provided here.

Previously, feature update of Windows 10 had to be manually installed using the method described at:

https://support.symantec.com/en_US/article.HOWTO125875.html

This process required the Symantec Endpoint Encryption administrator to manually update systems or use deployment software to automatically update systems in place.

The Symantec Endpoint Encryption 11.2.1 MP1 and later installer leverages "Windows Setup Automation" to create the `SetupConfig.ini` file and configures this file to use encryption drivers for the upgrade process.

The support for Windows feature update through Windows Update is enabled by default with `WINSETUPAUTOMATION` set to `1`.

During installation, if you had disabled this feature by setting `WINSETUPAUTOMATION` = 0, you can later enable this feature. To enable this feature, the Symantec Endpoint Encryption administrators need to follow steps provided here while installing or upgrading to Symantec Endpoint Encryption 11.3.1.

Before you install Symantec Endpoint Encryption 11.3.1 with support for Windows 10 feature update through Windows Updates

Before installing Symantec Endpoint Encryption 11.3.1, here are some details you need to know about the Windows feature update and Symantec Endpoint Encryption:

- Install or upgrade to Symantec Endpoint Encryption 11.3.1 before the Windows feature update initiates. Else the Windows feature update may fail.
- This feature is applicable only on a computer with Drive Encryption installed. This feature is not applicable on a computer with only Removable Media Encryption installed.
- This feature is applicable only for Windows 10 and later.
- This feature is not compatible with Symantec Encryption Desktop installed along with Symantec Endpoint Encryption client on a computer.
  Workaround: Exit PGPTray.exe and any other PGP services before Windows feature update initiates. For more details, refer to the Microsoft article:
  https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/windows-setup-enable-custom-actions

Installing or upgrading to Symantec Endpoint Encryption 11.3.1 to enable Windows feature update

1. If you want to overwrite the existing value of `WINSETUPAUTOMATION`, then run the following command to install or upgrade to Symantec Endpoint Encryption 11.3.1 on a computer to enable or disable the Windows feature update.

   ```
   msiexec /i SEE_installer.msi WINSETUPAUTOMATION=<x> /l*v installation.log
   ```

   where `<x> = 1` to enable the Windows feature update,

   or `<x> = 0` to disable the Windows feature update.

2. Restart the computer.

   The `SetupConfig.ini` file is created at the following path:

   ```
   %systemdrive%\Users\Default\AppData\Local\Microsoft\Windows\WSUS\
   ```

   NOTE

   If an existing instance of the `SetupConfig.ini` file is present on the computer, it is overwritten after you install the Symantec Endpoint Encryption client with `WINSETUPAUTOMATION=1`.

   The `installation.log` file is also created.

Enabling Windows feature update after installing Symantec Endpoint Encryption 11.3.1

If you install or upgrade to the Symantec Endpoint Encryption client with `WINSETUPAUTOMATION=0` or without the `WINSETUPAUTOMATION` parameter, you can later change to `WINSETUPAUTOMATION=1`.

To change `WINSETUPAUTOMATION=1`, edit the following registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Encryption Anywhere\Hard Disk]

WINSETUPAUTOMATION=dword:1
```

Later, if you do not want to leverage the Windows feature update through Windows Update, then do the following:

- Edit the registry and set `WINSETUPAUTOMATION=0`.
- Restart the system.
  The contents (reflectdriver and PostOobe keys) of the `SetupConfig.ini` file are automatically deleted.

Troubleshooting

If the Windows feature update fails, then administrator can retry the feature update after taking the following actions:

- Manually edit the `SetupConfig.ini` file to include `\Copylogs <folder for logs>`.
- Clean the `SoftwareDistribution` folder.

Installing the Windows Password Reset Utility on a client computer

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 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

If you installed the Symantec Endpoint Encryption Client to a custom installation folder, make sure that you install the Windows Password Reset Utility in the same location.

To install the Windows Password Reset Utility MSI file on a client computer

1. Navigate to the folder in which you saved the Windows Password Reset Utility client MSI file that you want to install.
2. Double-click the MSI file.
3. When prompted to restart, click **Yes** to restart your system and complete the installation.

Creating a Windows Password Reset Utility installation package

Deploying client installers using the command line

Using the command line to deploy Symantec Endpoint Encryption Client enables you to specify an output log file that you can use to troubleshoot any installation problems.

NOTE

If you run the Symantec Endpoint Encryption Client installation package to modify the number of features that are installed on the client computer, first ensure that the disk is already fully encrypted or decrypted. If disk encryption or decryption is in progress, wait until the operation is complete.

To run the Symantec Endpoint Encryption Client installer

1. Copy the installation .MSI file to the local hard disk of the computer on which you want to run the installer.
   - 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.
2. Depending on the version of Microsoft Windows, do one of the following:
   - **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**. If you are prompted, enter the credentials of a domain administrator account.
   - **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.
3. In the Command Prompt window, enter one of the following commands:
   - To perform a fresh installation:
     ```
     MSIEXEC /i "[path]\msifile" /l*v "[logpath]\logfile"
     ```
   - To modify an existing setup by installing an additional feature:
     ```
     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.

4. (Optional) You can specify the following additional command line parameter to the installation command to prevent the installation from terminating if there is pending restart on the system:

   ```
   PRE_INSTALL_REBOOT_CHECK=NO
   ```

   By default, to protect the system, the installation terminates if there is a pending restart.

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

Where to find more information about deploying clients

For information about creating client installers, and deploying clients, see the Symantec Endpoint Encryption Management Server Online Help.

Using the Symantec Endpoint Encryption Management Server Configuration Manager

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.

Symantec Endpoint Encryption Management Server Configuration Manager

Database Configuration page

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

Table 8: 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.
Database name	This field displays the name of the Symantec Endpoint Encryption database.
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*.

Option	Description
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 Server authentication. When you choose **SQL Server authentication**, the **Web application pool identity** field appears. (See the description below in this table.)
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.
Web application pool identity	When you choose **SQL Server authentication**, the **Web application pool identity** field appears. The default is your Network Service account. You may leave this default, if you are using a single server for your deployment. If you are using multiple servers with a load balancer, customize the field to a Windows domain account. (Use the same account across all servers.) A custom account lets the web-based Help Desk Recovery console access Active Directory for a user's User Group association. **Note:** If you will be using Kerberos authentication for the web-based Help Desk Recovery console, prior to setting the **Web application pool identity**, read "Preparing the environment for Kerberos authentication" in the *Symantec Endpoint Encryption Installation Guide* or the *Symantec Endpoint Encryption Upgrade Guide*. **To create a custom account** 1. Next to the **Web application pool identity** field, click **Change**. 2. In the Set Custom Web Application Identity pop-up window, the **Network Service account** radio button remains selected by default. Select **Custom account**. – In the **User name** field, type a Windows domain account (domain\user name). – In the **Password** field, type a password. Select the **Show password** option to display the characters that you type. – Click **OK**.
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.

About using the Symantec Endpoint Encryption Management Server Configuration Manager

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 9: 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.
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.
Enable Windows Authentication	Select this field: • If you have Removable Media Encryption installed and you will be distributing the RME Workgroup Key to Active Directory computers. • For client communication to utilize more secure Windows Authentication instead of Basic Authentication. **Note:** Selecting this field causes the **Custom SPN configuration** field to appear.
Custom SPN configuration	Select this field if the Service Principal Name has been configured to the **Web application pool identity** Windows account, which is defined on the Database Configuration page. The configuration should have taken place at the Windows command line, using the `setspn` command, during Kerberos authentication preparations. All preparations to setting this field are defined in "Preparing the environment for Kerberos authentication" in the *Symantec Endpoint Encryption Installation Guide* and the *Symantec Endpoint Encryption Upgrade Guide*. The selection of this **Custom SPN configuration** setting is required for Kerberos authentication. **Note:** If you have set a custom SPN configuration and thus have modified the website settings, on **Next** or **Save**, you are instructed to reset IIS. See the **Next/Save** option below for the reset command. Database Configuration page

Option	Description
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. This HTTPS communication is also used to securely transmit a pre-provisioned FileVault user credentials to the Mac system.
Disable TLS 1.0 and TLS 1.1	This field lets you enable or disable TLS 1.0 and TLS 1.1, the less powerful versions of the TLS communication protocol. Note that: • The default value for this field is that it is selected (protocols are disabled). The default protocol is TLS 1.2. • If TLS 1.0 and TLS 1.1 are already enabled during an upgrade to v11.3, they remain enabled. • If you have older clients checking in with the server, enable the protocols for backward compatibility. • If you change this setting, upon clicking **Save**, you receive a success message instructing you to reboot. • This field does not appear as an installation setting; it is only available for later configuration, using the Configuration Manager.
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. **Important**: If you selected **Custom SPN configuration**, upon a successful save, you are notified that you must reset IIS. At a Windows elevated prompt, execute this command: `iisreset.exe`. While IIS resets, any communication to the server is disrupted.

About using the Symantec Endpoint Encryption Management Server Configuration Manager

Symantec Endpoint Encryption Management Server Configuration Manager

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 10: 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.

About using the Symantec Endpoint Encryption Management Server Configuration Manager

Symantec Endpoint Encryption Management Server Configuration Manager

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 11: 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.
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.

About using the Symantec Endpoint Encryption Management Server Configuration Manager

Symantec Endpoint Encryption Management Server Configuration Manager

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.

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 12: 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: **Note:** ""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: **Note:** http://www.symantec.com/docs/HOWTO110233

About using the Symantec Endpoint Encryption Management Server Configuration Manager

Symantec Endpoint Encryption Management Server Configuration Manager

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 13: 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 do the following: • 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 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.

Server Role	Snap-in Access	Function
	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.
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	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.
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.

Server Role	Snap-in Access	Function
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.

Server Roles Configuration page

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 supersede 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:

18. On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.
19. Select **Server Roles** from the list on the left of the screen.
20. On the **Server Roles Configuration** page, switch the **Manage Server Roles** toggle to **On**.
21. 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.

22. Under **Select location**, select **This Computer**.
23. On the **Select User** page or the **Select Group**, click **Search** to view a list of all available local users or local groups.
24. Click **Search**.
25. 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.
26. Click **Show Selected** to view the list of users or groups that you selected for configuration.
27. Click **Next**.
28. 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.
29. Click **Show Selected** to view the list of endpoint groups that will be assigned to the selected users or groups.
30. Click **Next**.
31. 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 supersede 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.
32. Click **Next**.
33. On the **Summary** page, review the configured settings, and then click **Finish**.
34. 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 14: 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.
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**.

Add Users / Groups wizard - Select User

Add Users / Groups wizard - Select Group

About using the Symantec Endpoint Encryption Management Server Configuration Manager

Symantec Endpoint Encryption Management Server Configuration Manager

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 15: 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**.
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.

About using the Symantec Endpoint Encryption Management Server Configuration Manager

Symantec Endpoint Encryption Management Server Configuration Manager

Certificates and Token Software Settings

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 16: 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 17: 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.

Recommended token software configuration

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 18: 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.

Recommended token software configuration

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.

Using Symantec Endpoint Encryption authentication certificates

Using Removable Media Encryption certificates

Uninstalling Symantec Endpoint Encryption

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. Go to **Control Panel > Programs and Features**.
3. (Optional) If **Windows Password Reset Utility** is 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

8. 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.

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 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.

NOTE
If you need to restrict local users from uninstalling the Symantec Endpoint Encryption client, you may enable the **Allow Client Uninstallation for SYSTEM User only** Advanced Settings option, and allow only the SYSTEM user to uninstall the Symantec Endpoint Encryption client.

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

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

Uninstalling the Symantec Endpoint Encryption client software using the Control Panel

Uninstalling the Symantec Endpoint Encryption client software using the command line

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 11.3.1, 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 11.3.1 directly, for example, you did not use a GPO to upgrade to version 11.3.1.
- 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 11.3.1 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.

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

Deploying uninstallation scripts using Group Policy Objects

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 11.3.1 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. About uninstalling the Symantec Endpoint Encryption client

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 11.3.1 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.

About uninstalling the Symantec Endpoint Encryption client

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 using an account of a user who is part of the Active Directory Group defined in the **Management Agent - Advanced Setting: ma.uninstall.adGroupName** having sufficient privileges to uninstall software.

   For details, see Configuring the Management Agent - Advanced Settings policy options.

2. To access the Control Panel, do one of the following:
   - 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 **Windows Password Reset Utility** is 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

Privileged group user(s) or members of the specified Active Directory group user defined at **Management Agent - Advanced Settings: ma.uninstall.adGroupName**, can use the command prompt to uninstall one or more Symantec Endpoint Encryption features from a single computer. The results of the uninstallation are saved in a log file that you specify.

Configuring the Management Agent - Advanced Settings

NOTE

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

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 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
     ```
5. (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
     ```
6. (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
     ```
7. (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 Mac 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
   ```

Copyright Statement


Symantec
A Division of Broadcom