Getting Started

About Symantec Endpoint Encryption

Symantec™ Endpoint Encryption is comprised of the Drive Encryption functionality, the Removable Media Encryption functionality, and a Management Agent.

- Drive Encryption
  The Drive Encryption functionality ensures only authorized access to the data that is stored on hard disks. This functionality helps safeguard enterprises from data loss or breach in case of theft or accidental damage to laptops or PCs.
- Removable Media Encryption
  The Removable Media Encryption functionality protects data available on standard, off-the-shelf removable storage devices. As part of Symantec Endpoint Encryption, Removable Media Encryption helps prevent the unauthorized physical or logical access that jeopardizes the confidentiality of the data on a removable storage device. Removable Media Encryption provides file-based encryption using passwords or certificates and supports external hard drives, USB flash drives, and portable devices. An Access Utility to enable access to encrypted files on unmanaged systems (Microsoft Windows or Mac OS X) is also provided.
- Management Agent
  Management Agent includes all of the functionalities that are used across Symantec Endpoint Encryption, such as authentication methods and settings, registering users and setting up client administrator accounts and information.

If you are using Microsoft Windows Server 2008

For Symantec Endpoint Encryption Management Agent to appear properly on Windows Server 2008 R2, you must install the Aero Desktop theme.

Note: You must have administrator privilege to install the Aero Desktop theme.

To know how to install the Aero Desktop theme, see the Microsoft documentation.

How Removable Media Encryption works

Removable Media Encryption allows your organization to protect against loss of data arising from the misplacement or theft of removable media. Removable Media Encryption secures data in one of the following ways:

- By allowing no access to removable media
- By allowing only read access to removable media
- By automatically encrypting all of the files that you write to a removable media
- By automatically encrypting files according to Symantec Data Loss Prevention
- By encrypting the files that exist on a removable media whenever requested

Your organization determines which of these measures should be effective on your computer. These preventative measures reduce the likelihood of data breach incidents.

Removable Media Encryption uses complex algorithms to scramble the information that exists in a file into an indecipherable series of cryptic characters using a key. These

data would be available only to those who possess the key that is required to decrypt the encrypted information. Therefore, a key is required for both encryption and decryption of data. For Removable Media Encryption, this key is either derived from a password or a certificate.

If your computer is configured to encrypt files on a removable media, you can set a default password or default certificate for your computer. When a default password or a default certificate is specified, Removable Media Encryption does not prompt you to authenticate each time it encrypts or decrypts a file.

Based on the administrative policies of Symantec Endpoint Encryption Management Server, your policy administrator specifies whether you can encrypt a file using a password, a certificate, or both.

- When your encryption method is a password, you can encrypt a file only with a password.
- When your encryption method is a certificate, you can encrypt a file only with a certificate.
- When your encryption method is a password or a certificate or both, you must consider the following:
  - To encrypt files only with a password, set your default password in the Management Agent. Do not set a default certificate. You can then encrypt your files only with a password in the future.

    Note: When you have only one certificate in your personal store, Removable Media Encryption selects the certificate as your default certificate. Removable Media Encryption then encrypts your files with both the default password you have specified and the certificate it selects from the personal store. To encrypt files only with a password, ensure that you either have multiple certificates or you do not have a certificate in your personal store.
  - To encrypt files only with a certificate, set your default certificate in the Management Agent if you have multiple certificates in your personal store. Do not set a default password. You can then encrypt your files only with a certificate in the future.
  - To encrypt files with both a password and a certificate, set a default password and a default certificate in the Management Agent. Once the default password and default certificate are set, you always have to encrypt your files with a password and a certificate. To encrypt your files only with a password or a certificate, request your Client Administrator to change the configuration.

Note: If neither of the encryption method is specified, Removable Media Encryption prompts you to set a default password when have multiple certificates and you attempt to encrypt a file. When you copy a file to your removable media, the **Set Default Password** dialog box appears prompting you to set your default password.

When you right-click a file on a removable device connected to your client computer, Symantec Endpoint Encryption analyzes the encryption status of the file. Based on the encryption status of the file, Symantec Endpoint Encryption provides the Encrypt or Decrypt option. When you select and right-click multiple files, Symantec Endpoint Encryption displays both the Encrypt and Decrypt options for you take a required action.

Based on the policies that your administrator enables for your computer, you can also encrypt your files using a group key. A group key might be useful when a group of trusted users at work frequently share files using a removable media. Contact your client administrator to know about your group key.

Removable Media Encryption also provides you the ability to encrypt or decrypt files on the computers that do not have the Removable Media Encryption functionality. Your policy administrator can enable a policy to copy a utility on your removable media when you connect the media to your computer. With this utility, you can get most of the features of Removable Media Encryption even on the computers that do not have Removable Media Encryption installed.

Note: To use a removable device on a VMware ESXi system, disable the HotAdd/HotPlug capability. For information on how to disable this capability, see the VMware ESXi documentation or knowledge base.

See "Encrypting a file or folder with Removable Media Encryption" on page 4.

See "Decrypting an encrypted file or folder with Removable Media Encryption" on page 5.

Viewing the Removable Media Encryption policies

If you are a client user and have administrative privileges on your computer, you can view the Removable Media Encryption policies that are enabled for your computer.

To view the Removable Media Encryption policies

1. On the **Start** menu, click **All Programs** > **Symantec Endpoint Encryption** > **SEE Management Agent**.
2. On the **Removable Media** tab, click **Policy** to the view the list of active Removable Media Encryption policies.

Setting or changing a default password

A default password eliminates the need for Removable Media Encryption to prompt you for a password each time it encrypts or decrypts a file on your computer. Based on the policies that are configured for your client computer, the default password must meet certain password complexity requirements.

Every time you change a default password, the new password is used for the files that you encrypt after changing it. The default passwords that are used for encryption are automatically cached for each login session. When you change the default password, Removable Media Encryption requires the old default password to decrypt the files that were encrypted using it. Removable Media Encryption receives the old password from the cache until you log off from your computer, after which the password gets wiped off from the cache. When you log in again and try to decrypt the files that were encrypted with your old default password, Removable Media Encryption prompts you to provide the password.

To avoid remembering multiple passwords, you can copy all of the files from your removable media to another location before you change your default password. You can then change the default password and copy your files back on to the media. All your files, therefore, are encrypted with the new default password.

The **Set Default Password** dialog box appears when your encryption method is a password and you have not set a default password for file encryption. The **Set Default Password** dialog box also appears when the encryption method configured for your computer is a password or a certificate or both. The dialog box appears when you either have multiple certificates in your personal store or you do not have a certificate in your personal store.

To set or edit a default password from Management Agent

1. On the **Start** menu, click **All Programs** > **Symantec Endpoint Encryption** > **SEE Management Agent**.
2. On the **Removable Media** tab, click **Password**.
3. Under **Default Password**, do the following:
   - In the **Password** box, type your default password. As you type your password, the icon next to **Show Password** displays the minimum complexity that you need to consider to create a default password successfully.
   - In the **Confirm Password** box, type the default password again.
   - In the **Hint** box, type a clue to help you remember your default password.

   You can also check **Show Password** to see the characters of your default password as you type in the **Password** and **Confirm Password** box.
4. Click **Save**.

To set a default password from the Set Default Password dialog box

1. In the **Password** box, type your default password.
2. In the **Confirm** box, type the default password again.

   You can also check **Show password** to see the characters of your default password as you type in the **Password** and **Confirm** box. You can click the icon next to the **Confirm** box to view the minimum complexity that you need to consider while creating your password.
3. Click **OK** to save the default password for your computer.

See "Encrypting a file or folder with Removable Media Encryption" on page 4.

See "Decrypting an encrypted file or folder with Removable Media Encryption" on page 5.

Setting or changing a default certificate

Removable Media Encryption uses the designated default certificate to encrypt files and does not prompt you to provide certificates every time you encrypt or decrypt a file.

You can set or change the default certificate using the Management Agent. You can also set the default certificate from the **Set Default Certificate** dialog box. Removable Media Encryption finds all valid certificates that you have in your personal certificate store and displays a list of certificates. You can select a certificate from the list and set it as your default certificate.

Note: The **Set Default Certificate** dialog box appears when there are two or more certificates in your personal certificate store that match the criteria of certificate selection.

When you change a default certificate, Removable Media Encryption uses the new certificate for the files that you encrypt after changing it. Removable Media Encryption also requires the old certificate to decrypt the files that were encrypted using it. Removable Media Encryption uses the old certificate for decryption until the certificate is available in your personal certificate store. If you delete the old certificate from your personal certificate store, Removable Media Encryption prompts for the old certificate.

To set or edit the default certificate using the Management Agent

1. On the **Start** menu, click **All Programs** > **Symantec Endpoint Encryption** > **SEE Management Agent**.
2. On the **Removable Media** tab, click **Certificate**.
3. In the list of certificates available under **Default Certificate**, select the certificate that you want to set as your default certificate for file encryption.

   You can view the details of the certificate in the **Name**, **Issued to**, **Issued by**, and **Expires** columns before you select a certificate.
4. Click **Save**.

To set the default certificate from the Set Default Certificate dialog box

1. In the list of certificates, select the certificate that you want to set as your default certificate.
2. Click **OK** to save the default certificate for your computer.

See "Encrypting a file or folder with Removable Media Encryption" on page 4.

See "Decrypting an encrypted file or folder with Removable Media Encryption" on page 5.

Encrypting a file or folder with Removable Media Encryption

To protect data on your removable media, Removable Media Encryption encrypts the files or folders you write to the removable media. Administrative policies of Symantec Endpoint Encryption Management Server control the file encryption, and based on the policies in effect, your files can be encrypted in one of the following ways:

- Encryption of only those files that are written after the installation of Removable Media Encryption on the computer

  Note: Removable Media Encryption automatically encrypts any new file that you create on a removable storage device. When you modify an existing file on a removable storage device, Removable Media Encryption identifies the temporary file that gets created during the modification of the file as a new file. Removable Media Encryption, therefore, encrypts the modified file when it is saved. However, for those files that do not create any temporary file during its modification, such as the .txt file, you can create a new copy of the existing files on the removable storage device to encrypt them
- Encryption of files based on Symantec Data Loss Prevention

Your policy administrator can also control whether or not you can select and encrypt existing files or folders on your removable media.

Removable Media Encryption encrypts files based on the encryption policy that are enabled for your client computer. Based on the administrative policies, Removable Media Encryption also exempts a few file types from encryption that your policy administrator specifies for your computer.

Note: Removable Media Encryption automatically encrypts any exempted Microsoft Office file if it is modified and saved on a removable storage device that is connected to the client computer. The file type exemption policy is not applicable in such a case.

Each time Removable Media Encryption attempts to encrypt a file, it requires a key for encryption. This key is derived either from a password or a certificate. Based on the policy that is enabled for your computer, Removable Media Encryption encrypts the file with a password, a certificate, or both. You can set a default password or default certificate for your computer before writing files or folders to your removable media. After you set a default password or certificate, Removable Media Encryption uses the default password or default certificate to encrypt files or folders on your computer.

When you write a file or folder to a removable media, Removable Media Encryption prompts you to set the default password or default certificate for your computer. This prompt appears when Removable Media Encryption does

not find a default password or default certificate for your computer.

When you encrypt a large file or folder, Removable Media Encryption displays a progress bar to indicate that the encryption is in progress. After the encryption completes, the file gets a golden lock icon overlay to indicate the encryption status.

To encrypt a file or folder on a removable media that is connected to a computer that does not have Removable Media Encryption installed, use Removable Media Access Utility. For more information on how to use Removable Media Access Utility to encrypt files or folders, see the *Removable Media Access Utility Online Help*.

To encrypt a file or folder that you write to a removable media

1. Insert the removable media into your computer on which Removable Media Encryption is installed.
2. Copy the files or folders from your computer and paste them to the removable media.
3. Do one of the following:
   - If the **Set Default Password** dialog box appears, set a default password for your computer.
   - If the **Set Default Certificate** dialog box appears, select a certificate from the list to set it as the default certificate for your computer.
4. When encryption is complete, confirm that the files have a golden lock icon overlay on them.

To encrypt a file or folder on a removable media connected to your computer

1. On the removable media, browse to the location of the file or folder that you want to encrypt.
2. Select the file or folder.

   You can also select multiple files or folders for encryption.
3. Right-click the files or folders and click **Symantec Encryption** > **Encrypt**.
4. Do one of the following:
   - If the **Set Default Password** dialog box appears, set a default password for your computer.
   - If the **Set Default Certificate** dialog box appears, select a certificate from the list to set it as the default certificate for your computer.
5. When the encryption completes, confirm that the files have a golden lock icon overlay on them.

See "Decrypting an encrypted file or folder with Removable Media Encryption" on page 5.

See "Setting or changing a default password" on page 3.

See "Setting or changing a default certificate" on page 3.

Decrypting an encrypted file or folder with Removable Media Encryption

Each time Removable Media Encryption attempts to decrypt a file, it requires a key for decryption. This key is derived either from the password or the certificate that was used to encrypt the file. When Removable Media Encryption does not find a default password or default certificate that was used for encryption, it prompts you to provide the password or certificate. However, when the default password or default certificate is set, Removable Media Encryption decrypts the files or folders without any prompts.

Note: If a file is both password-encrypted and certificate-encrypted, you can decrypt the file using either a password or a certificate.

When you decrypt a large file or folder, Removable Media Encryption displays a progress bar to indicate that the decryption is in progress. After the decryption completes, the golden lock icon overlay that indicates the encryption status of the file disappears.

To decrypt a file on a removable media that is connected to a computer that does not have Removable Media Encryption installed, use Removable Media Access Utility. For more information on how to use Removable Media Access Utility to decrypt files or folders, see the *Removable Media Access Utility Online Help*.

To decrypt an encrypted file or folder that you copy from a removable media

1. Insert the removable media into your computer on which Removable Media Encryption is installed.
2. Copy the files or folders from your removable media and paste them to the desired location on your computer.

3 If Removable Media Encryption prompts you to enter the password that was used for encryption, enter the password in the **Password** box, and click **OK**.

4 When the decryption completes, confirm that the golden lock icon overlay disappears from the files.

To decrypt an encrypted file or folder on a removable media connected to your computer

1 On the removable media, browse to the location of the file or folder you want to decrypt.

2 Select the files or folders.

You can also select multiple files or folders for decryption.

3 Right-click the files or folders and click **Symantec Encryption** > **Decrypt**.

4 If Removable Media Encryption prompts you to enter the password that was used for encryption, enter the password in the **Password** box, and click **OK**.

5 When the decryption completes, confirm that the golden lock icon overlay disappears from the files.

See "Encrypting a file or folder with Removable Media Encryption" on page 4.

See "Setting or changing a default password" on page 3.

See "Setting or changing a default certificate" on page 3.

Recovering an encrypted file

Based on the administrative policies of Symantec Endpoint Encryption, Removable Media Encryption encrypts a file with a recovery certificate in addition to the password or certificate that is set for the computer. The recovery certificate provides an option to recover an encrypted file in case the password or the certificate that was used for encryption is lost.

When your administrator enables this option, Removable Media Encryption encrypts a file with the public key of the recovery certificate. As a client administrator, you can use the copy of the recovery certificate that includes the private key to recover the encrypted file.

To recover an encrypted file on computer with Removable Media Encryption installed

1 Insert the token or the smart card that contains the recovery certificate into the client computer.

2 Authenticate the token or the smart card software, if prompted.

3 Insert the removable media that contains the file to be recovered.

4 Drag the encrypted file to a desired location on your computer.

Removable Media Encryption decrypts the file using the private key of the recovery certificate.

Getting Technical Support

For additional assistance using Symantec Endpoint Encryption Removable Media Encryption functionality, contact the help desk or the local administrator of your organization.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com