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.

Working with Drive Encryption

Symantec Endpoint Encryption client software provides an interface to:

- View the encryption status of your hard disk partitions.
- Determine if the check-in enforcement policy is enabled for your computer.
- Verify the last time your computer had checked in with Symantec Endpoint Encryption Management Server, if at all.
- Force your computer to check in with Symantec Endpoint Encryption Management Server.

In addition to these, you can do the following:

- View the product version information.
- View the Symantec Endpoint Encryption functionalities that are installed on your computer.
- View the legal notice of the Symantec Endpoint Encryption functionalities.

Viewing the encryption status of your disks

Drive Encryption protects the data that are stored on your hard disk by encrypting it. Encryption is the process by which an algorithm renders data unreadable. Only those who possess the "key" can decrypt the data, thereby rendering it intelligible again.

The disks of your computer are configured to be encrypted automatically after Drive Encryption functionality is installed and the computer restarts. Encryption begins within about five minutes.

Note: If you have a Microsoft eDrive support - Opal v2 compliant drive installed and the self-encrypting drives

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.

Working with Drive Encryption

Symantec Endpoint Encryption client software provides an interface to:

- View the encryption status of your hard disk partitions.
- Determine if the check-in enforcement policy is enabled for your computer.
- Verify the last time your computer had checked in with Symantec Endpoint Encryption Management Server, if at all.
- Force your computer to check in with Symantec Endpoint Encryption Management Server.

In addition to these, you can do the following:

- View the product version information.
- View the Symantec Endpoint Encryption functionalities that are installed on your computer.
- View the legal notice of the Symantec Endpoint Encryption functionalities.

Viewing the encryption status of your disks

Drive Encryption protects the data that are stored on your hard disk by encrypting it. Encryption is the process by which an algorithm renders data unreadable. Only those who possess the “key” can decrypt the data, thereby rendering it intelligible again.

The disks of your computer are configured to be encrypted automatically after Drive Encryption functionality is installed and the computer restarts. Encryption begins within about five minutes.

Note: If you have a Microsoft eDrive support - Opal v2 compliant drive installed and the self-encrypting drives policy is enabled, then the disk encryption starts and completes in less than a minute.

You can continue to work normally during and after the encryption of your hard disk. All partitions should be encrypted, especially the Windows system partition.

The administrator can specify a policy to include or skip the encryption of unused disk space.

The administrator can also specify a policy to automatically encrypt all of the secondary disks on the client computer.

To view the encryption status of your disks and partitions

1. On the **Start** menu, click **All Programs** > **Symantec Endpoint Encryption** > **SEE Management Agent**.
2. On the **Internal Drives** tab, click **Drives**.
3. View the encryption status of your disks and partitions. The status can be one of the following:
   - **Encrypting**
     Indicates that the encryption of the disks and partitions is not complete. Along with this status, the page also displays the percentage of the disks and partitions already encrypted. Drive Encryption displays a progress bar for the partitions to indicate encryption progress.

     Note: To view the status of each partition on a particular disk, expand the disk.
   - **Encrypted** with a lock icon
     Indicates that the disks and partitions are fully encrypted.

     Note: If you have a Microsoft eDrive support - Opal v2 compliant drive installed and the self-encrypting drives policy is enabled, then the encrypted status of that drive appears as **Hardware Encrypted**. However, if the Opal drive partitions are not consistent with the range values for partitions, then the Opal drive is software encrypted. The status appears as **Encrypted**.
   - **Encryption has been paused**
     Indicates that the encryption of the disks and partitions is paused.
   - **Decrypting**
     Indicates that the decryption of the disks and partitions is not complete. Along with this status, the page also displays the percentage of decryption remaining for the disks and partitions. Drive Encryption displays a progress bar for the partitions to indicate decryption progress.
   - **Not Encrypted** with an unlock icon
     Indicates that the disks and partitions are not encrypted. This status appears for a disk or partition that was encrypted previously but now is fully decrypted. The **Not Encrypted** status also appears for a disk or partition that has never been encrypted.
   - **Decryption has been paused**
     Indicates that the decryption of the disks and partitions is paused.

See "Authenticating in preboot to access your encrypted computer" on page 2.

See "Communicating with Symantec Endpoint Encryption Management Server" on page 4.

Authenticating in preboot to access your encrypted computer

About preboot authentication

Drive Encryption needs a set of credentials before it lets you access your protected hard drive. After Drive Encryption is installed, Drive Encryption silently registers you when you successfully log on with your Windows credentials. Drive encryption uses your Windows password or PIN to register you for preboot authentication. Drive Encryption registers every user that logs on to the computer with a different Windows credential.

After registration, each time you restart your computer, you are prompted for credentials before Windows loads.

- If your policy administrator enabled single sign-on, you log on to preboot once with your Windows user name and password or PIN. You directly access your computer without authenticating to Windows.
- If single sign-on is not enabled, you log on once to preboot and once to Windows. For both logons, you use your Windows credentials.

If your computer has a check-in policy with lockout enforcement and has not communicated with the Symantec Endpoint Encryption Management Server, you are locked out of your computer at preboot. Ask your client administrator for help.

Note: The preboot authentication screen is not displayed if Autologon is in effect.

policy is enabled, then the disk encryption starts and completes in less than a minute.

You can continue to work normally during and after the encryption of your hard disk. All partitions should be encrypted, especially the Windows system partition.

The administrator can specify a policy to include or skip the encryption of unused disk space.

The administrator can also specify a policy to automatically encrypt all of the secondary disks on the client computer.

To view the encryption status of your disks and partitions

1 On the **Start** menu, click **All Programs** > **Symantec Endpoint Encryption** > **SEE Management Agent**.

2 On the **Internal Drives** tab, click **Drives**.

3 View the encryption status of your disks and partitions. The status can be one of the following:

  - **Encrypting**
    Indicates that the encryption of the disks and partitions is not complete. Along with this status, the page also displays the percentage of the disks and partitions already encrypted. Drive Encryption displays a progress bar for the partitions to indicate encryption progress.

    Note: To view the status of each partition on a particular disk, expand the disk.

  - **Encrypted** with a lock icon
    Indicates that the disks and partitions are fully encrypted.

    Note: If you have a Microsoft eDrive support - Opal v2 compliant drive installed and the self-encrypting drives policy is enabled, then the encrypted status of that drive appears as **Hardware Encrypted**. However, if the Opal drive partitions are not consistent with the range values for partitions, then the Opal drive is software encrypted. The status appears as **Encrypted**.

  - **Encryption has been paused**
    Indicates that the encryption of the disks and partitions is paused.

  - **Decrypting**
    Indicates that the decryption of the disks and partitions is not complete. Along with this status, the page also displays the percentage of decryption remaining for the disks and partitions. Drive Encryption displays a progress bar for the partitions to indicate decryption progress.

  - **Not Encrypted** with an unlock icon
    Indicates that the disks and partitions are not encrypted. This status appears for a disk or partition that was encrypted previously but now is fully decrypted. The **Not Encrypted** status also appears for a disk or partition that has never been encrypted.

  - **Decryption has been paused**
    Indicates that the decryption of the disks and partitions is paused.

See "Authenticating in preboot to access your encrypted computer" on page 2.

See "Communicating with Symantec Endpoint Encryption Management Server" on page 4.

Authenticating in preboot to access your encrypted computer

About preboot authentication

Drive Encryption needs a set of credentials before it lets you access your protected hard drive. After Drive Encryption is installed, Drive Encryption silently registers you when you successfully log on with your Windows credentials. Drive encryption uses your Windows password or PIN to register you for preboot authentication. Drive Encryption registers every user that logs on to the computer with a different Windows credential.

After registration, each time you restart your computer, you are prompted for credentials before Windows loads.

- If your policy administrator enabled single sign-on, you log on to preboot once with your Windows user name and password or PIN. You directly access your computer without authenticating to Windows.
- If single sign-on is not enabled, you log on once to preboot and once to Windows. For both logons, you use your Windows credentials.

If your computer has a check-in policy with lockout enforcement and has not communicated with the Symantec Endpoint Encryption Management Server, you are locked out of your computer at preboot. Ask your client administrator for help.

Note: The preboot authentication screen is not displayed if Autologon is in effect.

Supported languages for the preboot authentication screen

The preboot authentication screen supports the following languages: English, French, German, Japanese, and Spanish. By default, the preboot authentication screen is displayed in the language that your administrator configures.

Note: Japanese is not a supported language for the preboot authentication screen on UEFI-based systems.

Unsupported characters in preboot

Preboot authentication does not support certain ALT characters such as ALT+155. These are the special characters that appear when you press the ALT key with your number pad. To avoid preboot authentication issues, do not use ALT characters in your user name or password.

Startup and preboot authentication screens

Once you have registered, each time you turn on your computer, you must authenticate.

Note: A startup screen may appear first. To proceed to the preboot authentication screen, press Enter.

On the authentication screen:

- If you registered with a password, enter your password here.
- If you registered with a token, press F7, and then authenticate with your PIN.

Authenticating to preboot using a password

To authenticate to preboot using a password

1. On the preboot authentication screen, enter the following information:
   - In the **User Name** box, type your Windows user name.

     You can use the TAB key to navigate to another text box.

     Note: By default, asterisks appear for each character that you type. Alternatively, your cursor randomly steps through the spaces. If you want to change your preboot data entry behavior, contact your client administrator. The administrator can use the command line to change the behavior.

   - In the **Password** box, type your Windows password. Press F3 to hide or show the password characters.

     Press F2 to select a second keyboard layout. Press F8 to toggle between the current and previously selected keyboard layouts.

   - In the **Domain** box, use the arrow keys to navigate to the appropriate domain name.
2. Press Enter.

Authenticating to preboot using a token

To authenticate to preboot using a token

1. On the preboot authentication screen, press F7.
2. Type your PIN in the **Token PIN** box.
3. Press Enter.

See "Selecting additional keyboard layouts for preboot authentication" on page 3.

See "Regaining access to your computer after a communication lockout" on page 8.

See "Gaining access to your computer using Help Desk Recovery" on page 7.

See "Using Drive Encryption Self-Recovery when you forget your password" on page 6.

Selecting additional keyboard layouts for preboot authentication

Different keyboard layouts can have different mappings between characters, potentially causing problems when you enter your passphrase to authenticate. Select the keyboard layout that most closely maps to the keyboard you are using. Ensure that you to use the same layout each time you authenticate.

If your system is running in BIOS mode, the active keyboard layout is indicated above the **User Name** box. If your system is running in UEFI mode, the active layout is indicated at the bottom of the preboot authentication screen.

You can select and use two keyboard layouts at a time. By default, the secondary keyboard layout is English (US). When you select a new keyboard layout, it becomes the active (primary) layout that you can immediately use to enter your password. The keyboard layout that you had been using then becomes the secondary layout.

You can press F8 to toggle between the selected keyboard layouts. You can replace either layout as many times as necessary.

Note: Changing the keyboard layout does not affect the characters that you have already typed in the **Password** box.