# Contents

1. Introduction ................................................................................................................................. 1
   Overview ........................................................................................................................................ 1

2. Registration Prompts ..................................................................................................................... 3
   Overview ........................................................................................................................................ 3
   The Prompts .................................................................................................................................. 3
   Multiple Users ............................................................................................................................... 3
   Grace Restarts Available ............................................................................................................... 4
   Registration Mandate .................................................................................................................... 4

3. Administrator Client Console ......................................................................................................... 5
   Overview ........................................................................................................................................ 5
   Logon ............................................................................................................................................. 5
   Basics ........................................................................................................................................... 5
   Password ....................................................................................................................................... 5
   Token ............................................................................................................................................. 6
   Home ............................................................................................................................................. 7
   Navigation ..................................................................................................................................... 8
   Mouse Navigation ......................................................................................................................... 8
   Keyboard Navigation .................................................................................................................... 9
   Registered Users .......................................................................................................................... 10
   Removable Storage ....................................................................................................................... 11
   About .......................................................................................................................................... 13

4. File Recovery .................................................................................................................................. 14
   Overview ........................................................................................................................................ 14
   Recovery Procedure ...................................................................................................................... 14
   Basics ........................................................................................................................................... 14
   With Removable Storage Access Utility on PC .......................................................................... 14
   From a Removable Storage-Protected Computer ....................................................................... 15

Appendix A. Token Usage & Error Messages .................................................................................... 16
   Overview ........................................................................................................................................ 16
   Token Usage .................................................................................................................................. 16
   Insertion ......................................................................................................................................... 16
   Recognition .................................................................................................................................... 16
   Error Messages .............................................................................................................................. 17

Glossary ............................................................................................................................................. 19
Index ........................................................................................................................................... 22
Figures

Figure 2.1—Registration Prompt, Multiple Users ................................................................. 3
Figure 2.2—Registration Prompt, Grace Restarts Available .................................................. 4
Figure 2.3—Registration Prompt, Mandate ........................................................................ 4
Figure 3.1—Administrator Client Console Logon, Password .................................................. 5
Figure 3.2—Administrator Client Console Logon, Token ......................................................... 6
Figure 3.3—Select Certificate .............................................................................................. 7
Figure 3.4—Administrator Client Console, Home ................................................................. 7
Figure 3.5—Administrator Client Console, User Interface Elements .................................... 8
Figure 3.6—Administrator Client Console, Registered Users ................................................. 10
Figure 3.7—Administrator Client Console, Removable Storage ............................................. 11
Figure 3.8—Administrator Client Console, About ............................................................... 13
Figure 4.1—Removable Storage Access Utility, Decrypt To Location, with Recovery Certificate .................................................. 15
1. Introduction

Overview

Symantec Endpoint Encryption Removable Storage allows your organization to protect against loss of data arising from the misplacement or theft of removable storage devices.

Removable Storage secures data in one of the following ways:

- By allowing no access to removable storage devices,
- By allowing only read access to removable storage devices,
- By automatically encrypting all files written to or accessed on removable storage devices,
- By automatically encrypting all files written to removable storage devices,
- By automatically encrypting files per Symantec Data Loss Prevention for Endpoint,
- By automatically encrypting data written to CD/DVD media, and/or
- By encrypting files written to a removable storage device on user demand,

These preventative measures reduce the likelihood of data breach incidents.

Removable Storage enforces access and encryption policies on devices that use USB or Firewire ports and attach a file system.

This Guide assumes that the Symantec Endpoint Encryption Management Server, Symantec Endpoint Encryption Manager, and Symantec Endpoint Encryption clients have already been deployed. For instructions on creating client installation packages, refer to the Installation Guide. For information relevant to policies refer to the Policy Administrator Guide. For information about the end user experience, refer to the User Guide.

This Guide discusses:

- Symantec Endpoint Encryption administrator roles;
- Best practices;
- Registration prompts;
- The Administrator Client Console;
- Recovery of Removable Storage–encrypted files; and
- Token usage.

Symantec Endpoint Encryption Roles

Policy Administrator

Policy Administrators perform centralized administration of Symantec Endpoint Encryption. Using the Manager Console and the Manager Computer, the Policy Administrator:

- Updates and sets client policies.
- Runs reports.

Access to Symantec Endpoint Encryption snap-ins can be restricted on a per snap-in basis, giving the domain or higher-level administrator flexibility when assigning specific Policy Administrator duties.
**Client Administrator**
Client Administrators provide local support to Symantec Endpoint Encryption users.

Client Administrator accounts are created and maintained from the Symantec Endpoint Encryption Manager. Client Administrator accounts are managed entirely by Symantec Endpoint Encryption and independent of Windows, allowing Client Administrators to support users who are not a part of an Active Directory domain.

Client Administrators may be configured to authenticate with either a password or a token. Client Administrator passwords are managed from the Manager Console and cannot be changed at the Client Computer. This single-source password management allows Client Administrators to remember only one password as they move among many Client Computers.

Client Administrators are always able to log on to the Administrator Client Console. The ability to unregister users is a privilege that Client Administrators may or may not have.

Client Administrators should be trusted in accordance with their assigned level of privilege.

The Client Administrator is also responsible for recovering Removable Storage–encrypted files when the user has forgotten their password and a Recovery Certificate was used. This responsibility is not controlled by privilege level.

Each Client Computer must have one default Client Administrator account. The default Client Administrator account has a high privilege level and authenticates using a password. Up to 1024 total Client Administrator accounts can exist on each Client Computer.

Client Administrators must register as a user to make use of removable storage devices at the Removable Storage–protected workstation.

**User**
At least one user is required to register with Symantec Endpoint Encryption on each Client Computer. A wizard guides the user through the registration process, which involves a maximum of five screens. The registration process can also be configured to occur without user intervention. Users will not be able to access their removable storage devices until they have registered.

To ensure the success of this product in securing your encrypted assets, Symantec recommends that you do not define users as local administrators or give users local administrative privileges.

**Best Practices**

**Trusted Software**
Firewalls and anti-virus software should be installed on Client Computers to protect against viruses and secure computers against invasive software that arrives over the network, such as a trojan horse. File sharing, peer-to-peer networks, and FTP servers are not recommended. Network logon scripts must be approved scripts. If remote access to stored data is allowed, users with remote access must be required to authenticate.

**Local Administrator Rights**
Users should not be defined as local administrators or given local administrative privileges.

**Password Security**
Both Client Administrators and registered users should not share passwords and avoid writing them down. A user’s awareness must include being aware of others watching over their shoulder as they type and they should be told to change their passwords if this has happened.

**Frequent Information Backup**
User data as well as log files should be backed up on a regular basis. This will allow users to recover from theft or hard disk failure. Audit logs can help reveal patterns that occur over time, such as a series of failed logon attempts. The user data backups should be physically protected or encrypted.
2. Registration Prompts

Overview
Unless you register as a user, each time you log on to the Removable Storage-protected computer, you will be greeted by a registration prompt. Three different types of registration prompts will be displayed, according to the following conditions:

- At least one user has registered.
- Grace restarts remain.
- No user is registered and grace restarts have expired.

If no users have registered with Symantec Endpoint Encryption and the designated number of grace restarts has expired, you will be forced to register. Until a user registers, access to Windows will be denied.

Otherwise, registration prompts will be optional and can be dismissed. However, you will be prevented from using removable storage devices from the workstation until you do register as a user.

If you decide to register, see the User Guide for information on the registration process.

If you register for a registered user account, you will have two valid accounts on the Client Computer. Your Client Administrator account will allow you to access the Administrator Client Console. Your registered user account will allow you to access the User Client Console and to use removable storage devices.

You can always unregister your registered user account later using the Administrator Client Console. Each Client Computer has a maximum number of registered users allowed. Depending on the maximum number of user accounts allowed and the number of users of the workstation in question, you may want to unregister your account to free up a slot for someone else to register.

The Prompts

Multiple Users
If at least one user has already registered to Symantec Endpoint Encryption, you will be prompted to register on an optional basis.

If you need to use removable storage devices from this workstation, click Register Now. Refer to the User Guide for registration instructions.

Otherwise, click Don’t Ask Me Again. You will not be prompted to register again unless you attempt to launch the User Client Console from the Start menu.
Grace Restarts Available
Grace restarts are the number of times users can reboot without having to register. The following figure shows a sample of a message you would receive if grace restarts have been provided and no users are currently registered with Symantec Endpoint Encryption.

If you need to use removable storage devices from this workstation, click Register Now. Refer to the User Guide for registration instructions.

Otherwise, click Cancel to dismiss the prompt.

Registration Mandate
Once grace restarts expire, or if no grace restarts were provided, you will be forced to register if no users have registered yet.

Until someone registers with Symantec Endpoint Encryption, no access to Windows will be available. You have two choices. You can either pass the Client Computer to the designated user of the machine and have them register, or you can register as a user yourself. If you need to use removable storage devices from this workstation, you will need to register.

If you choose to pass the computer to the designated user, click Log Off Windows.

Otherwise, click Register to begin the registration process. See the User Guide for registration instructions.
3. Administrator Client Console

Overview
The Administrator Client Console is available once Windows has loaded and allows you to view the following workstation-specific information:

- The users that have registered to Symantec Endpoint Encryption;
- Which Symantec Endpoint Encryption products are installed and their version numbers; and
- What access and encryption policies are being enforced by Removable Storage.

In addition, you may be able to unregister users.

To start the Administrator Client Console, click on the Start menu, point to Symantec Endpoint Encryption Client, then select Symantec Endpoint Encryption Administrator Client.

If the User Client Console is open, you will be prompted to close it, as both consoles cannot be running simultaneously.

💡 If you are assisting a visually impaired user who uses JAWS to navigate Windows, shut JAWS down prior to launching the Administrator Client Console.

Logon

Basics
If you log on with a token, see “Token” on page 6. If you log on with a password, see the next section.

Password
If your account uses a password to authenticate, enter your credentials in the Client Administrator Logon panel.

![Image of Administrator Client Console Logon, Password](image.png)

Figure 3.1—Administrator Client Console Logon, Password
Select **Password** from the **Authentication method** menu, type your account name in the **Account name** field, enter your Symantec Endpoint Encryption password in the **Password** field, then click **Log On**.

If your password is not correct, the logon will fail. Check your password and re-enter the information. Your Policy Administrator may have implemented a logon delay to occur when one or more incorrect logon attempts are made. This delay helps protect the computer against password-guessing attacks. If such a setting or policy is in place and you or someone else triggers that restriction, the **Account name** and **Password** fields become unavailable. A message informs you that the number of allowed password attempts has been exceeded and a running countdown displays how long you must wait before you can try again.

If your authentication succeeds, you will be given access to the Administrator Client Console. Skip to “Home” on page 7.

**Token**

**Token Insertion**
The Logon panel prompts you to insert your token.

If your token is already inserted, skip to the next section; otherwise, insert your token. For proper insertion of your token and for a description of token behavior when the token is being read, refer to Appendix A “Token Usage” on page 16. Make sure the token has been read before you proceed with authentication.

**PIN Entry**
In the **Account name** field type the account name given to you by your Policy Administrator. In the **PIN** field, type your PIN, then click **Log On**. Do not remove the token until authentication completes.

If your authentication succeeds, you are given access to the Administrator Client Console. Skip to the section “Home” on page 7.

If you encounter errors with your token, certificate, or PIN, refer to Appendix A “Error Messages” on page 17.

**Certificate Selection**
If the **Select Certificate** dialog appears, continue reading; otherwise, skip to the next section “Home” on page 7.
Select your Symantec Endpoint Encryption certificate by clicking on the appropriate row, then clicking **OK**.

If you select a certificate that is not valid, you will receive an error message. If you don’t know which certificate to choose, contact your administrator.

**Home**

The Administrator Client Console opens to the Home panel, which appears with an enabled navigation pane.
**Navigation**

The Administrator Client Console is divided into several sections. The following figure uses callouts to identify the elements.

The sections are as follows:

- The banner displays the product logo and the account name of the Client Administrator that logged on to this Administrator Client Console.
- The navigation pane contains hyperlinks to all panels. A panel loads into the main pane when its link is clicked. The links include Registered Users, Removable Storage, and an About panel.
- The main pane changes in response to your clicking a link in the navigation pane. For example, if you click Registered Users, the main pane displays the Registered Users panel.
- The Quick Help pane provides context-sensitive help based on the location of your mouse. See the next section for how to display Quick Help.

Standard visual indicators are used to identify the user interface element that has focus. A dotted line outlines the link, button, check box, or icon having focus. Highlighting or a blinking cursor indicates the input field that has focus. In Figure 3.5, Registered Users has focus.

You may navigate the Administrator Client Console using a mouse or using the keyboard.

**Mouse Navigation**

If you are using a mouse to navigate the Administrator Client Console:

- To load a panel, click the desired hyperlink in the navigation pane; the panel loads into the main pane.
To display Quick Help, click the help icon 📘. The Quick Help pane appears. To close the Quick Help pane, click the help icon again.

**Keyboard Navigation**

**Direct Access**

Use the keys listed in Table 3.1 to directly access Administrator Client Console panels.

<table>
<thead>
<tr>
<th>To Go To This Panel</th>
<th>Press This Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Users</td>
<td>ALT+U</td>
</tr>
<tr>
<td>Removable Storage</td>
<td>ALT+R</td>
</tr>
<tr>
<td>About</td>
<td>ALT+B</td>
</tr>
</tbody>
</table>

**TAB Key Access**

To navigate the Administrator Client Console:

- Press the TAB key to move among the screen elements.
- To load a panel, press the TAB key to the desired link in the navigation pane, then press ENTER. The panel loads into the main pane and focus moves to the panel.
- To display Quick Help, press the TAB key until the focus is on the help icon 📘, then press ENTER or the SPACEBAR. To close the Quick Help pane, press ENTER or the SPACEBAR again. Note that Quick Help applies at the panel level; context-sensitive Quick Help is available only when using a mouse.
- To select a check box, press the TAB key to place focus on the box, then press the SPACEBAR. To toggle off the selection, press the SPACEBAR again.
- To activate a button, press the TAB key to place focus on the button, then press ENTER or the SPACEBAR.

The TAB key follows standard user-interface behavior:

- Tabbing order within each panel is top to bottom, left to right.
- To move down, press the TAB key; to move up, press SHIFT+TAB.
- To scroll, use the UP ARROW key and the DOWN ARROW key.

When you use the TAB key to navigate, you may need to press the key more than once to place the focus on the next desired link, input field, button, or icon, depending on the location of the current focus.
**Registered Users**

Use the Registered Users panel to view Symantec Endpoint Encryption accounts on a computer. You may also be able to unregister users, if your privileges permit. To open the Registered Users panel, click *Registered Users* in the navigation pane. The Registered Users panel appears, populated with the registered user accounts on that computer.

If you have the right to unregister users, a check box will be available beside each user name. When you unregister a user, the user’s Symantec Endpoint Encryption account is deleted and that user can no longer log on to the User Client Console or access removable storage devices from the workstation.

Reasons for unregistering a user include:

- Employee departure;
- Workstation or laptop reallocation; and/or
- Registered user account maximum approaching or reached.

Select the check box next to the user account(s) that you want to unregister. The *Unregister Selected Users* button becomes available. Click *Unregister Selected Users*. The account is removed and the *Number of registered users* is decremented.

A policy may exist that mandates unregistration of users who do not log on for a specified number of days. Inactive users will be automatically unregistered and will no longer be visible in the users list.
Removable Storage
The Removable Storage panel will inform you of the policies in place on this machine. From the navigation pane click Removable Storage.

![Removable Storage Panel](image)

Figure 3.7—Administrator Client Console, Removable Storage

Removable Storage is either allowing no access to removable storage devices, permitting read-only access to removable storage devices, or allowing read and write access to removable storage devices. If Removable Storage is allowing read and write access, it is enforcing one of the following encryption policies:

- No encryption,
- Automatic encryption of all files written to or accessed on removable storage devices,
- Automatic encryption of all files written to removable storage devices,
- Automatic encryption of data written to CD/DVD media using the Removable Storage CD/DVD Burner application,
- Automatic encryption of files as per Symantec Data Loss Prevention for Endpoint, and/or
- Encrypting files written to a removable storage device on user demand.
The Removable Storage panel informs you of the policies in place on this machine. For example, in Figure 3.7, a read-write access policy is in place, with new files written to removable storage devices being automatically encrypted.

### Table 3.2—Removable Storage Panel Messages and Policies in Effect

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
<th>Policy in Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Symantec Endpoint Encryption policy on this computer does not allow access to removable storage devices.</td>
<td>This computer will not allow files to be read from or written to removable storage devices.</td>
<td>Access Policy: No Access</td>
</tr>
<tr>
<td>The Symantec Endpoint Encryption policy on this computer allows read-only access to removable storage devices when a registered user is logged on to Windows.</td>
<td>If the user currently logged on to Windows has registered with Symantec Endpoint Encryption, the user will be able to read files from removable storage devices, but cannot write files to removable storage devices.</td>
<td>Access Policy: Read Only</td>
</tr>
<tr>
<td>The Symantec Endpoint Encryption policy on this computer allows read and write access to removable storage devices when a registered user is logged on to Windows.</td>
<td>If the user currently logged on to Windows has registered with Symantec Endpoint Encryption, the user will be able to both read files from and write files to removable storage devices.</td>
<td>Access Policy: Read and Write</td>
</tr>
<tr>
<td>All files written to or accessed on these devices are automatically encrypted.</td>
<td>If the user currently logged on to Windows has registered with Symantec Endpoint Encryption, when the user attempts to access removable storage device files, the files will be encrypted. An informative warning message will be displayed first, providing the user with an option to avoid accessing and thereby encrypting the removable storage device files. Files written to removable storage devices will also be encrypted by Removable Storage.</td>
<td>Encryption Policy: Encrypt All</td>
</tr>
<tr>
<td>New files written to these devices are automatically encrypted.</td>
<td>File written to removable storage devices will be encrypted by Removable Storage.</td>
<td>Encryption Policy: Encrypt New</td>
</tr>
<tr>
<td>New files written to these devices are not encrypted.</td>
<td>Files on removable storage devices will not be encrypted by Removable Storage.</td>
<td>Encryption Policy: Do Not Encrypt</td>
</tr>
<tr>
<td>Files written to removable storage devices will not be encrypted, but files written to CD/DVDs will be encrypted.</td>
<td>New files written to CD/DVD using the Symantec Endpoint Encryption CD/DVD burner application will be encrypted.</td>
<td>Encryption Policy: CD/DVD only</td>
</tr>
<tr>
<td>Files are encrypted as per Symantec Data Loss Prevention for Endpoint.</td>
<td>If the user currently logged on to Windows has registered with Symantec Endpoint Encryption, files stored on removable storage devices (except for CD/DVD) are encrypted per policy set through the Symantec Data Loss Prevention for Endpoint product.</td>
<td>Encryption Policy: Encrypt per Symantec DLP for Endpoint</td>
</tr>
<tr>
<td>The Policy allows users to decide about the default encryption about the files written to devices.</td>
<td>If the user currently logged on to Windows has registered with Symantec Endpoint Encryption, the user can select whether the default action is to encrypt new files, or not to encrypt new files written to a removable storage device.</td>
<td>Encryption Policy: User Choice</td>
</tr>
</tbody>
</table>
Table 3.2—Removable Storage Panel Messages and Policies in Effect (Continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
<th>Policy in Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following groups of file types are exempted from encryption: Audio</td>
<td>Removable Storage will not attempt to encrypt files belonging to the group(s) specified in the panel. See the User Guide for the file types included in each group.</td>
<td></td>
</tr>
<tr>
<td>Video</td>
<td>Image</td>
<td></td>
</tr>
<tr>
<td>The Symantec Endpoint Encryption policy on this computer allows Removable Storage users to set a device session default password for each inserted removable storage device while it is connected. The password is automatically deleted when the removable device is removed or when the user logs off of Windows.</td>
<td>This policy allows users to set a default password for each removable storage device while it is connected. Removable Storage deletes the password when the device is removed or when the user logs off of Windows. Password aging does not apply, but any defined password management requirements do.</td>
<td>Default Passwords Policy: Allow device session default passwords</td>
</tr>
</tbody>
</table>

About

Use the About panel to find out which version of Framework and Removable Storage the computer is running. To open the About panel, click About.

The build number associated with a given version number is accessible as a Tooltip. Hover your mouse over the version number; the build number appears. The build number can be used to see if patches have been applied.

💡 From time to time, a service pack number (SPn) is appended to the build string, indicating that this is not a major release but an update that fixes existing problems and in some cases delivers product enhancements.

Click Show legal notice to see the legal notices associated with each product.
4. File Recovery

Overview
To recover files encrypted under a given Recovery Certificate, you must have the copy of the Recovery Certificate that includes the private key.

The procedure can be performed using either:

- A PC not protected by Removable Storage and the Removable Storage Access Utility, or
- A Removable Storage–protected computer.

If you are using the Removable Storage Access Utility, it must be from a computer that does not have Removable Storage installed. The Removable Storage Access Utility is not supported for use on Client Computers that have Removable Storage installed.

Recovery Procedure

Basics
Obtain the copy of the Recovery Certificate that includes the private key. Import this copy of the Recovery Certificate into the local certificate store of the computer that you plan to use to achieve recovery. This can be accomplished using several different methods, such as:

- Insert the token or smart card that contains the Recovery Certificate with the private key. Authenticate to the token or smart card software if prompted.
- Manually import the Recovery Certificate with the private key into the local certificate store.

Once the Recovery Certificate with the private key resides within the local certificate store, the procedure differs depending on whether or not the computer is protected by Removable Storage. If the computer is protected by Removable Storage, skip to “From a Removable Storage–Protected Computer” on page 15. Otherwise, continue reading.

With Removable Storage Access Utility on PC
1. Launch the Removable Storage Access Utility from the removable device containing the files to be recovered.
2. Verify that the lock icon of the file or folder to be recovered is gold, indicating that the Recovery Certificate with the private key resides within the local certificate store.
3. Select the folder or file requiring decryption.
4. Right-click the folder or file, point to **Decrypt To**, and select **Location**.

![Figure 4.1—Removable Storage Access Utility, Decrypt To Location, with Recovery Certificate](image)

5. The **Browse For Folder** dialog appears. Browse to the desired location or create a new folder. Click **OK**. The folder or file is decrypted and written to the specified location.

**From a Removable Storage–Protected Computer**
1. Log on to the computer at the Windows prompt.
2. If you are prompted to register with Symantec Endpoint Encryption, ensure that you do so. Only registered users can access removable storage devices from Removable Storage–protected computers.
3. Insert the removable storage device containing the files to be recovered.
4. Verify that the lock icon of the file or folder to be recovered is gold, indicating that the Recovery Certificate with the private key resides within the local certificate store.
5. Drag the recovered files from the removable device to the location of your choosing, such as the local hard disk.
Appendix A. Token Usage & Error Messages

Overview
This appendix describes correct token insertion, and token behavior when information is being read from your token.

It also lists the error messages that you may encounter while using your token to authenticate to the Administrator Client Console and suggests actions that you can take in response to each error message.

Token Usage

Insertion
To insert your token, follow the instruction for the appropriate token type:

- **Smart card**—hold the card so that the side containing the gold chip is on top and the card end containing the chip is closest to the reader.

- **USB-based**—connect the USB-connector end of your token to a USB port or into a USB extension cable attached to your computer.

Recognition
Make sure that the token software recognizes your token before you remove it, by referring to the appropriate description below:

- **Aladdin eToken**—the red light on the token itself blinks while the token is being read; the icon in your Windows notification area does not change.

- **Common Access Card (CAC) and Personal Identity Verification (PIV)**—the icon in your Windows notification area shows just a reader when the token is not inserted, then adds a blue token when the token has been inserted and read.

- **RSA token**—the icon in your Windows notification area changes to include a plus sign.

- **SafeSign v2.1**—no visual sign appears in the Windows notification area; simply wait a few moments after token insertion.

- **Smart card**—the icon’s computer screen changes from black to blue while the icon’s golden token blinks, then returns to black when the blinking stops.

If your token or the reader has a light, it blinks when information from your token is being read. Wait until all blinking stops before taking the next action, such as clicking Log On. Do not remove the token until token reading is complete.

If you encounter token or certificate errors, continue reading.
# Error Messages

Table A.1 lists the error messages that may occur when you use a token to log on to the Administrator Client Console using the Logon panel with **Authentication Method** set to **Token**.

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Incorrect account name or PIN.</td>
<td>You entered an incorrect account name / PIN pair.</td>
<td>Click <strong>OK</strong> to dismiss the message. If you think you incorrectly typed your credentials, re-enter them then click <strong>Log On</strong>. If you are not sure what your account name is, check with your Policy Administrator. If you are not sure of your PIN, contact the person who manages your token. Excessive incorrect attempts to enter your account name / PIN could result in your PIN being blocked.</td>
</tr>
<tr>
<td>All</td>
<td>The PIN is blocked for this token. The token needs to be replaced or modified by a token administrator.</td>
<td>The number of remaining attempts on your token is zero.</td>
<td>Follow the instructions for getting assistance. Your PIN is blocked. The appropriate administrator will need to replace or modify your token.</td>
</tr>
<tr>
<td>All</td>
<td>The program could not log you on. The token was removed.</td>
<td>You removed the token immediately after clicking <strong>Log On</strong>.</td>
<td>Reinsert the token and leave it inserted until you are logged on to the Administrator Client Console.</td>
</tr>
<tr>
<td>All</td>
<td>A certificate validation error has occurred. The token needs to be replaced or modified by a token administrator.</td>
<td>Your token does not contain any certificate, your token contains an invalid certificate, or your PIN has expired.</td>
<td>Contact the appropriate administrator.</td>
</tr>
<tr>
<td>All</td>
<td>The certificate selection failed. The token may need to be replaced or modified by a token administrator.</td>
<td>The certificate could not be retrieved from the local certificate store.</td>
<td>Contact the appropriate administrator. Your token software is not configured to add your certificate(s) to the local Windows certificate store each time you insert your token.</td>
</tr>
<tr>
<td>All</td>
<td>A token error has occurred. The authentication process cannot continue.</td>
<td>The token is unknown or the reader is not supported.</td>
<td>Ask your Policy Administrator which token type was selected during product installation and if your token reader is on the list of supported token readers. If necessary, the appropriate administrator may need to replace your token, upgrade your token software, or provide you with a supported token reader.</td>
</tr>
</tbody>
</table>
The program could not log you on. Your credentials could not be verified.
The authentication process failed.
It is possible that your token does not contain any certificates or that it contains certificates that were not issued to you.
The token logon process failed for some reason other than those listed in this table. Make sure that the inserted token is the one that was issued for your Symantec Endpoint Encryption account. If it is not, remove the invalid token, insert the valid token, and try to log on again.
If you continue to receive this message, contact the appropriate administrator.

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>The program could not log you on. Your credentials could not be verified.</td>
<td>The authentication process failed. It is possible that your token does not contain any certificates or that it contains certificates that were not issued to you.</td>
<td>The token logon process failed for some reason other than those listed in this table. Make sure that the inserted token is the one that was issued for your Symantec Endpoint Encryption account. If it is not, remove the invalid token, insert the valid token, and try to log on again. If you continue to receive this message, contact the appropriate administrator.</td>
</tr>
</tbody>
</table>
# Glossary

**Authentication Method**  Specifies how registered users and Client Administrators authenticate to Symantec Endpoint Encryption. Methods include password, token, password and token, or automatic. If the Policy Administrator changes the authentication method, registered users may be forced to re-register.

**Authenti-Check**  Allows users on endpoints to recover from forgotten credentials without help desk assistance. The user authenticates with a set of up to three question-answer pairs. Authenti-Check is not available to Client Administrators.

**Autologon**  Allows Policy Administrators to remotely deploy software to computers protected by Full Disk. Software installations typically require several restarts, and Autologon allows pre-boot authentication to be bypassed, so that the computer does not require any credentials before loading Windows.

**Automatic Authentication**  Allows any registered user to launch the User Client Console. The registration process will be automatic and occur without user intervention—unless a registration password is required.

**Client Administrator**  Provides local support to Symantec Endpoint Encryption users. Their main functions include unregistering users and recovering Removable Storage–encrypted files. Client Administrators cannot change their own passwords or use any password-recovery methods. Client Administrators must register as a user to make use of removable storage devices at the Removable Storage–protected workstation.

**Client Database**  The client database consists of a series of volume files and is part of the Symantec Endpoint Encryption file system. Once the location of the client database files has been specified during the creation of the Client Computer installation packages and the installation has completed, these files must never be moved or disturbed.

**Device Session Default Password**  A password used to encrypt and decrypt files on a removable device, as long as the device is connected and the user is logged on to Windows. This password is intended for kiosk environments, where users share a Windows account yet require the convenience of a Default Password. Password aging does not apply. This password does not apply to CDs or DVDs.

**One-Time Password (OTP) Program**  The One-Time Password (OTP) Program allows users on Windows endpoints to recover from a forgotten password, PIN, or token with help desk assistance. Users can also use the OTP program to regain access to their Windows computer after it has been locked for a failure to communicate with the Symantec Endpoint Encryption Management Server. To complete the OTP process the user must contact the help desk.
<table>
<thead>
<tr>
<th><strong>Policy Administrator</strong></th>
<th>Performs centralized administration of Symantec Endpoint Encryption. The Policy Administrator updates and sets client policies, and also runs reports.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pre-Windows Environment</strong></td>
<td>The Pre-Windows environment loads upon reboot, before the Windows operating system. This environment helps protect the Client Computer’s hard disks by requiring authentication before a user gains access to Windows.</td>
</tr>
<tr>
<td><strong>Recovery Certificate</strong></td>
<td>Used to decrypt encrypted files when the user-provided credentials are not available, allowing organizations to recover from forgotten passwords and lost certificates. You will need two copies of the same Recovery Certificate, one with the private key and one without.</td>
</tr>
<tr>
<td><strong>Reg</strong></td>
<td>Without Private Key—the Recovery Certificate without the private key is deployed to clients using an installation package or a policy. Upon receipt, clients will encrypt files using the Recovery Certificate in addition to the credentials provided by the user.</td>
</tr>
<tr>
<td><strong>Reg</strong></td>
<td>With Private Key—the Recovery Certificate with the private key is exported using the P7B format. It should be stored in a safe, physically secure location. Symantec recommends exporting it to a token or smart card and then securing the token or smart card in a fire-proof vault.</td>
</tr>
<tr>
<td><strong>Registration</strong></td>
<td>During registration, users set their credentials so that they can authenticate in pre-Windows. In addition, users may be asked to set password recovery information. Registration may be configured to occur with or without the user’s intervention. The first user is required to register after the designated number of grace restarts has expired.</td>
</tr>
<tr>
<td><strong>Re-Registration</strong></td>
<td>Symantec Endpoint Encryption users may be required to re-register if a Policy Administrator issues a computer policy or installs an upgrade package that requires them to change their authentication method.</td>
</tr>
<tr>
<td><strong>Self-Extracting Executables</strong></td>
<td>A feature of Removable Storage that allows any user of a Symantec Endpoint Encryption Removable Storage–protected workstation to create encrypted self-extracting executables for secure transport. Self-extracting executables can be decrypted from any computer, without any need for Removable Storage or the Removable Storage Access Utility. The ability to produce self-extracting executables is prescribed by installation setting or policy on a per computer basis.</td>
</tr>
<tr>
<td><strong>Single Sign-On (SSO)</strong></td>
<td>If SSO is enabled, a user can authenticate once to the User Client Console in a Windows session, then close and relaunch the User Client Console without further authentication.</td>
</tr>
<tr>
<td><strong>Symantec Endpoint Encryption Framework</strong></td>
<td>Provides Symantec Endpoint Encryption–wide features, such as authentication methods and settings, as well as registered user and Client Administrator accounts and information.</td>
</tr>
<tr>
<td><strong>Symantec Endpoint Encryption Password</strong></td>
<td>Used by Client Administrators or Users to authenticate to the Administrator Client Console or User Client Console.</td>
</tr>
<tr>
<td><strong>Temporary Data Directory</strong></td>
<td>The CD/DVD Burner application will first attempt to store its temporary data directory on the drive of the operating system. It checks the TMP, the TEMP, and then the USERPROFILE environment variables in succession. It will use the first environment variable it finds. If none of these environment variables has been set, the CD/DVD Burner Application will use the Windows directory.</td>
</tr>
<tr>
<td><strong>Unregistration</strong></td>
<td>The removal of a Symantec Endpoint Encryption registered user account, either manually by a Client Administrator or automatically by policy.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>At least one user must register with Symantec Endpoint Encryption on each Windows Client Computer. A wizard guides the user through the registration process, which involves a maximum of five screens. The registration process can also be configured to occur without user intervention. Users Cannot access their removable storage devices until they have registered.</td>
</tr>
</tbody>
</table>
Index

A
access policy
  no access 1, 11, 12
  read and write 1, 11, 12
  read only 1, 11, 12
Administrator Client Console
  About 13
  logon
    delay 6
    password 5
    token 6
      multiple certificates 6
  Registered Users 10
  Removable Storage 11

B
best practices, list of 2

C
CD/DVD Burner application
  temporary data directory 21
  certificate
    token 6
Client Administrator 2
  single-source passwords 2

D
default passwords policy
  allow device session default passwords 13
Device Session Default Password 13

E
encryption policy
  CD/DVD only 1, 12
  do not encrypt 11, 12
  encrypt all 1, 11, 12
  encrypt as per Symantec DLP 1, 11
  encrypt CD/DVD only 11
  encrypt new 1, 11, 12
  encrypt on user demand 1, 11
  per DLP for Endpoint 12
  user choice 12

F
file recovery 1, 14
  with Removable Storage Access Utility 14
  with Symantec Endpoint Encryption Removable Storage 15
  focus 8, 9

G
grace restarts, definition 4

N
navigation
  direct access keys 9
  mouse 8
  TAB key 9

P
password
  Symantec Endpoint Encryption 6
  Policy Administrator 1, 6, 17

Q
Quick Help, use 8

R
Recovery Certificate
  private key 14
  registration 3
  Removable Storage Access Utility 14

S
Symantec Endpoint Encryption
  build numbers 13
  version numbers 13

token
  reader 16

U
user
  maximum number of 10
  registration 5
  unregistration 10
  viewing accounts of 10