<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Introduction</td>
</tr>
<tr>
<td>- Overview</td>
</tr>
<tr>
<td>- Important Concepts</td>
</tr>
<tr>
<td>- Encryption</td>
</tr>
<tr>
<td>- Keys</td>
</tr>
<tr>
<td>- Default Passwords and Default Certificates</td>
</tr>
<tr>
<td>- Icon Overlays</td>
</tr>
<tr>
<td>- Registration</td>
</tr>
<tr>
<td>- User Client Console</td>
</tr>
<tr>
<td>- Policy Administrators</td>
</tr>
<tr>
<td>- Client Administrators</td>
</tr>
<tr>
<td>Tips and Tricks</td>
</tr>
<tr>
<td>- Work Locally</td>
</tr>
<tr>
<td>- Save As Versus Save</td>
</tr>
<tr>
<td>- Double Encryption</td>
</tr>
<tr>
<td>Best Practices</td>
</tr>
<tr>
<td>- Password/PIN Strength</td>
</tr>
<tr>
<td>- Password/PIN Secrecy</td>
</tr>
<tr>
<td>- Trusted Software</td>
</tr>
<tr>
<td>- Backups</td>
</tr>
<tr>
<td>2. Registration, Re-Registration &amp; Default Password Expiration</td>
</tr>
<tr>
<td>- Overview</td>
</tr>
<tr>
<td>- Registration Prompts</td>
</tr>
<tr>
<td>- Basics</td>
</tr>
<tr>
<td>- Grace Restarts Available</td>
</tr>
<tr>
<td>- Registration Mandate</td>
</tr>
<tr>
<td>- Multiple Users</td>
</tr>
<tr>
<td>Registration Wizard</td>
</tr>
<tr>
<td>- Basics</td>
</tr>
<tr>
<td>- Registration Password</td>
</tr>
<tr>
<td>- Preferred Authentication Method</td>
</tr>
<tr>
<td>- Password Registration</td>
</tr>
<tr>
<td>- Token Registration</td>
</tr>
<tr>
<td>- Authenti-Check</td>
</tr>
<tr>
<td>- Completion</td>
</tr>
<tr>
<td>Re-Registration</td>
</tr>
<tr>
<td>Default Password Aging</td>
</tr>
<tr>
<td>- Basics</td>
</tr>
<tr>
<td>- Warning</td>
</tr>
<tr>
<td>- Expiration</td>
</tr>
<tr>
<td>3. User Client Console</td>
</tr>
<tr>
<td>- Overview</td>
</tr>
<tr>
<td>- Basics</td>
</tr>
<tr>
<td>- Launch</td>
</tr>
<tr>
<td>- Single Sign-On</td>
</tr>
<tr>
<td>Logon Panel</td>
</tr>
</tbody>
</table>

Symantec Endpoint Encryption Removable Storage
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basics</td>
<td>17</td>
</tr>
<tr>
<td>Password</td>
<td>18</td>
</tr>
<tr>
<td>Token</td>
<td>19</td>
</tr>
<tr>
<td>Authentication Assistance</td>
<td>20</td>
</tr>
<tr>
<td>Home Panel</td>
<td>21</td>
</tr>
<tr>
<td>Navigation</td>
<td>23</td>
</tr>
<tr>
<td>User Interface Elements</td>
<td>23</td>
</tr>
<tr>
<td>Mouse Navigation</td>
<td>24</td>
</tr>
<tr>
<td>Keyboard Navigation</td>
<td>24</td>
</tr>
<tr>
<td>Registered Users Panel</td>
<td>25</td>
</tr>
<tr>
<td>Account Settings, Password Panel</td>
<td>26</td>
</tr>
<tr>
<td>Basics</td>
<td>26</td>
</tr>
<tr>
<td>Single Sign-On Not Enabled</td>
<td>26</td>
</tr>
<tr>
<td>Single Sign-On Enabled</td>
<td>27</td>
</tr>
<tr>
<td>Account Settings, Token Panel</td>
<td>28</td>
</tr>
<tr>
<td>Basics</td>
<td>28</td>
</tr>
<tr>
<td>Token Change</td>
<td>28</td>
</tr>
<tr>
<td>Token Addition</td>
<td>29</td>
</tr>
<tr>
<td>Account Settings, Authenti-Check Panel</td>
<td>30</td>
</tr>
<tr>
<td>Removable Storage Panel</td>
<td>31</td>
</tr>
<tr>
<td>Removable Storage, Default Passwords Panel</td>
<td>34</td>
</tr>
<tr>
<td>Removable Storage, Certificates Panel</td>
<td>35</td>
</tr>
<tr>
<td>User Choice Panel</td>
<td>37</td>
</tr>
<tr>
<td>About Panel</td>
<td>38</td>
</tr>
<tr>
<td>4. File Encryption/Decryption</td>
<td>39</td>
</tr>
<tr>
<td>Overview</td>
<td>39</td>
</tr>
<tr>
<td>Pre-Existing Unencrypted Files</td>
<td>39</td>
</tr>
<tr>
<td>Encryption Prompts</td>
<td>40</td>
</tr>
<tr>
<td>Basics</td>
<td>40</td>
</tr>
<tr>
<td>Certificate(s)</td>
<td>42</td>
</tr>
<tr>
<td>Password/Certificate(s)</td>
<td>43</td>
</tr>
<tr>
<td>Decryption Prompts</td>
<td>44</td>
</tr>
<tr>
<td>Basics</td>
<td>44</td>
</tr>
<tr>
<td>Password</td>
<td>44</td>
</tr>
<tr>
<td>Certificate(s)</td>
<td>44</td>
</tr>
<tr>
<td>Password/Certificate(s)</td>
<td>45</td>
</tr>
<tr>
<td>On Demand Encryption</td>
<td>46</td>
</tr>
<tr>
<td>Basics</td>
<td>46</td>
</tr>
<tr>
<td>Right-Click File Encryption</td>
<td>46</td>
</tr>
<tr>
<td>Right-Click File Decryption</td>
<td>46</td>
</tr>
<tr>
<td>Two Files With Same Name.</td>
<td>47</td>
</tr>
<tr>
<td>5. Self-Extracting Executables</td>
<td>49</td>
</tr>
<tr>
<td>Overview</td>
<td>49</td>
</tr>
<tr>
<td>Self-Extracting Archive Encryption</td>
<td>49</td>
</tr>
<tr>
<td>Save Archive</td>
<td>49</td>
</tr>
<tr>
<td>Attach Archive</td>
<td>51</td>
</tr>
<tr>
<td>Modify Archive</td>
<td>53</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Self-Extracting Archive Decryption</td>
<td>57</td>
</tr>
<tr>
<td>Renaming Emailed Files</td>
<td>57</td>
</tr>
<tr>
<td>File Launch</td>
<td>58</td>
</tr>
<tr>
<td>Decryption Prompts</td>
<td>58</td>
</tr>
<tr>
<td>6. Removable Storage Access Utility</td>
<td>62</td>
</tr>
<tr>
<td>Overview</td>
<td>62</td>
</tr>
<tr>
<td>Basics</td>
<td>62</td>
</tr>
<tr>
<td>Launching the Utility</td>
<td>63</td>
</tr>
<tr>
<td>Device Default Password</td>
<td>63</td>
</tr>
<tr>
<td>Basics</td>
<td>63</td>
</tr>
<tr>
<td>Set or Modify from File Menu</td>
<td>64</td>
</tr>
<tr>
<td>Set or Modify from Password Decryption Prompt</td>
<td>65</td>
</tr>
<tr>
<td>Suspend</td>
<td>65</td>
</tr>
<tr>
<td>Reinstate</td>
<td>65</td>
</tr>
<tr>
<td>Decryption</td>
<td>66</td>
</tr>
<tr>
<td>Basics</td>
<td>66</td>
</tr>
<tr>
<td>Open</td>
<td>66</td>
</tr>
<tr>
<td>Decrypt to Location</td>
<td>66</td>
</tr>
<tr>
<td>Decryption Prompts</td>
<td>67</td>
</tr>
<tr>
<td>Encryption</td>
<td>69</td>
</tr>
<tr>
<td>Adding Files/Folders</td>
<td>69</td>
</tr>
<tr>
<td>Manual Initiation</td>
<td>70</td>
</tr>
<tr>
<td>Encryption Reminder</td>
<td>71</td>
</tr>
<tr>
<td>PC Encryption Prompt</td>
<td>72</td>
</tr>
<tr>
<td>Mac Encryption Prompt</td>
<td>73</td>
</tr>
<tr>
<td>File or Folder Delete</td>
<td>74</td>
</tr>
<tr>
<td>Clean Up Temp Files Prompt</td>
<td>74</td>
</tr>
<tr>
<td>7. CD-DVD Burner</td>
<td>76</td>
</tr>
<tr>
<td>Overview</td>
<td>76</td>
</tr>
<tr>
<td>Burning a Disc</td>
<td>76</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>76</td>
</tr>
<tr>
<td>Navigation</td>
<td>76</td>
</tr>
<tr>
<td>Appendix A. Multimedia File Types Excluded</td>
<td>78</td>
</tr>
<tr>
<td>Overview</td>
<td>78</td>
</tr>
<tr>
<td>Audio</td>
<td>78</td>
</tr>
<tr>
<td>Video</td>
<td>79</td>
</tr>
<tr>
<td>Image</td>
<td>81</td>
</tr>
<tr>
<td>Appendix B. Token Usage</td>
<td>83</td>
</tr>
<tr>
<td>Overview</td>
<td>83</td>
</tr>
<tr>
<td>Token Insertion</td>
<td>83</td>
</tr>
<tr>
<td>Token Recognition</td>
<td>83</td>
</tr>
<tr>
<td>Appendix C. Error Messages &amp; Prompts</td>
<td>84</td>
</tr>
<tr>
<td>Overview</td>
<td>84</td>
</tr>
<tr>
<td>Token Registration</td>
<td>84</td>
</tr>
<tr>
<td>User Client Console Token Logon</td>
<td>85</td>
</tr>
<tr>
<td>Removable Storage Service</td>
<td>86</td>
</tr>
</tbody>
</table>
User Guide

Contents

CD-DVD Burner Application ................................................................. 91
User Client Console ........................................................................... 98
Glossary ............................................................................................ 100
Index ................................................................................................. 103
Figures

Figure 2.1—Registration Prompt, Grace Restarts Available .............................................. 5
Figure 2.2—Registration Prompt, Mandate ........................................................................... 5
Figure 2.3—Registration Prompt, Multiple Users ................................................................. 6
Figure 2.4—Registration, Registration Password ............................................................... 7
Figure 2.5—Registration, Preferred Authentication Method .............................................. 8
Figure 2.6—Password Registration, Single Sign-On Enabled ........................................... 9
Figure 2.7—Password Registration, Account Password ..................................................... 10
Figure 2.8—Token Registration, PIN Entry .......................................................................... 11
Figure 2.9—Token Registration, Summary ........................................................................ 12
Figure 2.10—Token Registration, Select Certificate ............................................................ 12
Figure 2.11—Registration, Authenti-Check ........................................................................ 13
Figure 2.12—Registration Success ..................................................................................... 14
Figure 2.13—Sample Re-Registration Mandate .................................................................. 15
Figure 2.14—Default Password Expiration Warning ....................................................... 15
Figure 2.15—Default Password Expiration, During Windows Session .................................. 16
Figure 2.16—Default Password Expiration, Upon Windows Logon ..................................... 16
Figure 3.1—User Client Console Logon, Password ................................................................ 18
Figure 3.2—User Client Console Logon, Token ................................................................... 18
Figure 3.3—Token Logon, Select Certificate ....................................................................... 19
Figure 3.4—User Client Console Logon, Authenti-Check ................................................... 20
Figure 3.5—User Client Console, Home ............................................................................. 21
Figure 3.6—User Client Console, User Interface Elements ............................................... 23
Figure 3.7—User Client Console, Registered Users ............................................................. 25
Figure 3.8—User Client Console, Account Settings, Password, SSO Not Enabled ................ 26
Figure 3.9—User Client Console, Account Settings, Password, SSO Enabled ...................... 27
Figure 3.10—User Client Console, Account Settings, Token Panel with Existing Token .......... 28
Figure 3.11—User Client Console, Account Settings, Token Panel without Existing Token .... 29
Figure 3.12—User Client Console, Account Settings, Authenti-Check .................................. 30
Figure 3.13—User Client Console, Removable Storage ....................................................... 31
Figure 3.14—User Client Console, Removable Storage, Default Passwords ......................... 34
Figure 3.15—User Client Console, Removable Storage, Certificates .................................. 35
Figure 3.16—User Client Console, Removable Storage, Select Default Certificates ............. 36
Figure 3.17—User Client Console, Removable Storage, User Choice Panel ......................... 37
Figure 3.18—User Client Console, About .......................................................................... 38
Figure 4.1—Plaintext File Message ................................................................................... 39
Figure 4.2—Exempted Devices Message ........................................................................... 40
Figure 4.3—Encryption Password Prompt ......................................................................... 41
Figure 4.4—Encryption Certificate Prompt ........................................................................ 42
Figure 4.5—Encryption Password/Certificate Prompt ....................................................... 43
Figure 4.6—Decryption Password Prompt ......................................................................... 44
Figure 4.7—Decryption Certificate Prompt ....................................................................... 45
Figure 4.8—Sample PIN Prompt, Axalto ........................................................................... 45
Figure 4.9—Decryption Password/Certificate Prompt ....................................................... 45
Figure 5.1—Self-Extracting Archive, Encryption .................................................................. 49
Figure 5.2—Self-Extracting Archive, Encrypt, Rename, and Email ..................................... 51
Figure 5.3—Self-Extracting Archive, Decryption, Password Prompt .................................. 54
Figure 5.4—Self-Extracting Archive, Decryption, Certificate Not Available ......................... 54
Figure 5.5—Self-Extracting Archive, Decryption, Password/Certificate Prompt .................. 55
Figure 5.6—Self-Extracting Archive, Package Modifier ..................................................... 55
Figure 5.7—Self-Extracting Archive, Add Files .................................................................... 56
Figure 5.8—Self-Extracting Archive, Extractor ................................................................... 57
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 demand.

Your organization determines which of these measures will be in effect on your computer.

These preventative measures reduce the likelihood of data breach incidents.

Removable Storage is Section 508 compliant if Job Access with Speech (JAWS) is installed and running. JAWS will read the graphical user interface of Removable Storage aloud. A visually simplified User Client Console will be displayed if JAWS is running.

Important Concepts

Encryption
Encryption is the ancient art of exchanging secret messages. Love and war have driven the evolution of cryptography over the centuries.

Today, very complex algorithms are used to scramble information into an indecipherable series of cryptic characters. Only those in possession of the “key” can decrypt the data, thereby rendering it intelligible again.

Keys
The key, in the case of Removable Storage, is derived from either a password or a certificate. Both encryption and decryption require a key.

Default Passwords and Default Certificates
If your machine is configured to encrypt files on removable storage devices and/or CD/DVDs automatically, you can either provide a password or a certificate on a per file basis or set Default Password(s) and/or Default Certificate(s) to be used for all files.

Default Passwords and Default Certificates eliminate the need for Removable Storage to prompt you each time it encrypts a file. Furthermore, Default Passwords and Default Certificates reduce the need for Removable Storage to ask for a password when it attempts to decrypt a file.

For example, if you have Removable Storage installed both at home and at work, you may wish to set up your home and work machines to use the same Default Password(s) and/or Certificate(s). Removable Storage will not need to prompt you to encrypt or decrypt files shared between machines configured to use the same Default Password(s) or Default Certificate(s).
Default Password(s) and Certificate(s) might also be useful if you and other people at work frequently share files via removable storage devices. If you and these other users were to set the same Default or Session Default Password or Certificate(s), you would be able to share files without any prompts. So these should be users that you can trust with your removable storage device files.

Whether you have the ability to set up to three Default Password(s), and/or up to ten Default Certificates depends on your organization.

**Icon Overlays**
Removable Storage identifies encrypted files with lock icon overlays.

If Removable Storage has the key for the file, the lock will be golden 🏷️.

If Removable Storage doesn’t have the key, the lock will be red 🔄.

If the lock is red, Removable Storage will prompt you for the password or certificate that was used to encrypt the file when you try to open it.

**Registration**
Once Removable Storage has been installed on your machine, you will need to register with Symantec Endpoint Encryption before you can access any removable storage devices. During registration, you create your Symantec Endpoint Encryption account. At least one user must be registered on each workstation once a designated number of grace restarts has passed.

Registration is a highly configurable process, involving a maximum of five screens. Your administrator may also have configured it to occur silently, so that the process is completely transparent to you.

**User Client Console**
You may be prompted to enter your Symantec Endpoint Encryption password or PIN before you access the User Client Console. If your computer is set for automatic authentication or you have Single Sign-On (SSO), you will not have to log on to the User Client Console.

The User Client Console provides you with the ability to view and modify your Symantec Endpoint Encryption settings. At a minimum, you can use the User Client Console to:

- View the other users that have registered to Symantec Endpoint Encryption on your machine.
- Find out which Symantec Endpoint Encryption products are installed on your machine and their version numbers.
- See which policies are being enforced by Removable Storage.

In addition, you may be able to:

- Add or change your Symantec Endpoint Encryption password.
- Add or change the token you use to authenticate to Symantec Endpoint Encryption.
- Set or change your Authenti-Check questions and answers.
- Set or modify your Default Password(s) and/or Default Certificate(s).
- Change your automatic encryption setting.

**Policy Administrators**
The Policy Administrator performs centralized administration activities, such as defining installation settings and policies that are pushed out to Client Computers.
**Client Administrators**
The Client Administrator is your primary Symantec Endpoint Encryption administrator contact. The Client Administrator can help you if you forget your Symantec Endpoint Encryption password or are unable to decrypt a file.

**Tips and Tricks**

**Work Locally**
We recommend that you use your own hard drive as the primary place of storage for your files and removable storage devices as the means of transporting these files from one place to another. Copy files from a removable storage device to your hard drive before you begin to work on them. Once your work is complete, copy them to your removable storage device.

**Save As Versus Save**
Removable Storage will encrypt differently depending on whether you select Save or Save As from the File menu. If you select Save and the file was already encrypted, it will use the existing password and/or certificate(s) under which the file was encrypted. If you select Save As, it will use the Default Password(s) and/or Certificate(s) specified in the User Client Console or it will prompt you to enter a password and/or select a certificate.

This is good to remember if a fellow Removable Storage user lends you their removable storage device and you access a file on that device. If you select Save, they would be able to open that file more easily than if you select Save As. If you select Save As, you may need to tell them the password it was encrypted under, or provide them with your Default Certificate or the certificate you selected at the prompt, before they can open the file again.

**Double Encryption**
It might seem that encrypting a file twice would make it twice as secure.

But if you encrypt something once with a product from one vendor and a second time with a product from another vendor, you may never be able to decrypt it again.

Some removable storage devices offer encryption services of their own. If your administrator has configured your installation of Removable Storage to always encrypt, do not utilize any additional encryption services that may be offered by your removable storage device, as you may not be able to decrypt the data.

**Best Practices**

**Password/PIN Strength**
Define a password or PIN that you can remember, so that you don’t have to write it down. Try to choose passwords and PINs that are closer to the maximum length allowed rather than to the minimum length allowed. Include a variety of characters, including upper and lowercase letters mixed with numbers and special characters, if allowed. When you create a password, think of one that is hard to guess; for example, don’t use a commonly known fact, such as your spouse’s name, or a fact that can be easily researched, such as your mother’s maiden name.

**Password/PIN Secrecy**
You are responsible for your password or PIN’s security. Change your password or request a new PIN if you feel that your password or PIN may have become compromised. Some situations to be mindful of are:

- You wrote your password or PIN on a piece of paper but now you can’t find that paper.
- Someone looked over your shoulder and watched you type your password or PIN.
**Trusted Software**

Be familiar with the software that is authorized to run on your computer. Be careful if you download software from the Internet. This software could contain spyware, viruses, malware, Trojan horses, or worms. Also use caution when opening email attachments.

**Backups**

If your organization does not perform automated backups, you should do so yourself on a regular basis. This will allow you to recover from theft or hard disk failure. Store your backups in a physically secure location, such as a locked cabinet.
2. Registration, Re-Registration & Default Password Expiration

Overview
One of the first signs that Removable Storage has been installed may be a prompt for registration. If you are prompted to register, you are encouraged to do so as soon as possible, even if registration is optional. You will not be able to access your removable storage devices until you register.

You also may be prompted to re-register. This can occur if your organization is switching authentication methods.

Registration Prompts

Basics
After Removable Storage is installed and your computer reboots, if you haven’t registered already, you may be prompted to do so.

Grace Restarts Available
Grace restarts are the number of times you can reboot without having to register. If you were provided with grace restarts and have not used them all, the registration prompt will identify how many remain.

While you can click Cancel and continue working normally, it’s best to click Register Now and begin the registration process (“Registration Wizard” on page 6).

Registration Mandate
Once your grace restarts expire, or if your administrator did not give you any grace restarts, you will be forced to register. A prompt will be displayed, stating this mandate.

Figure 2.1—Registration Prompt, Grace Restarts Available

Figure 2.2—Registration Prompt, Mandate
Registration takes only a few moments. Click **Register** to begin the registration process (“Registration Wizard” on page 6).

If you can’t complete registration now, click **Log Off Windows**. The next time you boot up, you will receive the same registration mandate.

**Multiple Users**
If at least one user has already registered on this computer, you may be prompted to register on an optional basis.

Click **Register Now** to begin the registration process (see “Registration Wizard” on page 6).

If you click **Ask Me Later** or **Don’t Ask me Again**, you will be unable to access removable storage devices.

### Registration Wizard

**Basics**
The Registration wizard guides you through the registration process. This wizard is the same for both registration and re-registration. The steps in this process will vary according to how your computer has been configured.

If you click **Cancel** in the Registration Wizard, your Symantec Endpoint Encryption account will not be created. You will be prompted to confirm that you really want to cancel.

To display Quick Help, click the help icon 📖. The Quick Help pane appears. To close the Quick Help pane, click the help icon again.
**Registration Password**
You may need a password to begin the registration process. If you don’t see the Registration Password panel, you don’t need to enter a registration password. Skip to the next section (“Preferred Authentication Method” on page 7).

A registration password is a way for your administrator to limit the number of users allowed to register on this computer. The registration password is not your Symantec Endpoint Encryption password; the registration password admits you to the registration process.

You should have received this password ahead of time. If you do not have the password, call your help desk or click **Cancel**.

Otherwise, type the password and click **Next**.

If the password is accepted, the next panel in the registration process appears.

If the password is not accepted, a message appears and you will need to correct the password then click **Next** to resubmit it, or click **Cancel**. The **Back** button is not available.

**Preferred Authentication Method**
If your administrator has chosen to allow you to authenticate with either a password or a token and Single Sign-On is not enabled, the Preferred Authentication Method panel will be displayed. If the Preferred Authentication Method panel is not displayed, refer to the section that corresponds to your authentication method:

- If you authenticate with a password, skip to “Password Registration” on page 9.
- If you authenticate with a token, skip to “Token Registration” on page 10.
- If you don’t authenticate (automatic authentication), skip to “Completion” on page 14.
Select the method of authentication that you prefer and click Next. If you select **Password**, continue to the next section. If you select **Token**, skip to “Token Registration” on page 10.

💡 While the Registration Wizard will only escort you through your preferred authentication method, you can add a second method using the User Client Console at any time following registration.
Password Registration

Basics
The password registration process will vary according to whether or not you have Single Sign-On enabled.

Single Sign-On Enabled
If Single Sign-On is enabled, the Registration wizard will display the Single Sign-On panel. If you don’t see the Single Sign-On panel, skip to “Single Sign-On Not Enabled” on page 10.

![Password Registration, Single Sign-On Enabled](image)

The credentials associated with your Windows account will be used for your Symantec Endpoint Encryption account. Click Next to continue.
Single Sign-On Not Enabled

If Single Sign-On is not enabled, the Account Password panel will be displayed.

![Password Registration, Account Password](image)

The Account Password panel will display the account information of the user currently logged on to Windows.

Define a password that you can remember, so that you don’t have to write it down. Try to choose passwords that are closer to the maximum length allowed rather than to the minimum length allowed. Include a variety of characters, including upper and lowercase letters mixed with numbers and special characters, if allowed. When you create a password, think of one that is hard to guess. Avoid obvious choices, such as your spouse’s name and your mother’s maiden name.

Follow the guidelines shown below the Confirm password field, if any. The password must be within the Password length specified. The Symbols allowed parameter identifies which of the symbols on your keyboard may be included in the password. The Include at least field identifies the number of required symbols, uppercase letters, lowercase letters, and/or digits that your password must contain, if any.

Tab to or click on the Confirm password field and type your password again. Click Next.

If the password does not meet the requirements, the requirement that the password does not meet will be displayed in red. If the Password field and Confirm password field do not match exactly, the password fields turn red.

### Token Registration

**Basics**

Token registration may require up to three steps:

1. Token insertion (“Token Insertion” on page 11),
2. PIN entry (“Single Sign-On Not Enabled” on page 11),

*Token Insertion*

If your token was inserted when the Registration Wizard began, you do not see a token-insertion prompt panel. Skip to the next section (“Single Sign-On Not Enabled” on page 11).

Otherwise, you will be prompted to insert your token. For details about token insertion and errors, refer to Appendix B “Token Usage” on page 83.

*Single Sign-On Not Enabled*

If Single Sign-On is not enabled, you will be prompted to enter your PIN. If you aren’t prompted, skip to the next section (“Confirmation” on page 12).

Figure 2.8—Token Registration, PIN Entry

💡 The **User name** and **Domain** fields are filled from the information stored on your token.

Type your PIN in the **PIN** field, then click **Next**.
Confirmation
For both SSO and non-SSO accounts, the next registration panel confirms the token information that Symantec Endpoint Encryption will use to authenticate you.

![Token Registration, Summary](image)

Verify the information and click Next.

Certificate Selection
If the Select Certificate window does not appear, skip to the next section “Completion” on page 14.

![Select Certificate](image)

Select your Symantec Endpoint Encryption certificate by clicking on the appropriate row, then click OK. Skip to the next section.

If you don’t know which of the certificates listed are valid, contact the appropriate administrator.

If you receive an error message, refer to Appendix C “Token Registration” on page 84.
**Authenti-Check**

If you have Authenti-Check enabled, then you will see the Authenti-Check panel. If you don’t see this panel skip to the next section (“Completion” on page 14).

Authenti-Check is a self-help recovery tool that allows you to gain access to the User Client Console if you forget your password, PIN, or token. It can also be used if you get a new token and need to change tokens.

One Authenti-Check question is always required. Up to three questions may be required, depending on how your system is configured.

Questions identified as required must be entered and answered.

If a question is identified as optional, you are encouraged to enter a question and an answer. The more question-answer pairs you have, the more secure your User Client Console access is. For maximum security, enter three questions and three answers.

Sometimes your Policy Administrator predefines questions for you. These questions you cannot change and you must provide answers for.

Try to choose answers that other people cannot guess easily. Follow similar guidelines for your questions and answers as you would for your password. Create pairs that:

- Do not contain commonly known information,
- Are longer rather than shorter, and
- You can remember without writing down.
See Table 2.1 for examples of secure and less secure questions.

Table 2.1—Authenti-Check Sample Questions

<table>
<thead>
<tr>
<th>Secure</th>
<th>Less Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who was your favorite teacher?</td>
<td>What is your social security number?</td>
</tr>
<tr>
<td>Who was your childhood hero?</td>
<td>Where were you born?</td>
</tr>
<tr>
<td>What is the street name where your favorite relative lived?</td>
<td>What is your mother’s maiden name?</td>
</tr>
</tbody>
</table>

Do not let others watch you enter them. Unlike passwords, the question-answer pairs are not displayed as asterisks or dots on your screen; they display in plain text.

When you have entered all questions and answers, click the Next button to submit your information. If your questions and answers fall within established guidelines, your information will be accepted; otherwise, fields that contain errors are highlighted in red. Correct any highlighted information then click Next.

**Completion**
The final Registration panel notifies you that your Symantec Endpoint Encryption user account is active.

Click Finish to complete the wizard and dismiss the panel. This will result in the launch of the User Client Console. See Chapter 3 “User Client Console” on page 17 for information about using the User Client Console.
Re-Registration

Your Policy Administrator may dictate a change in your Symantec Endpoint Encryption authentication method either as part of an upgrade or by policy update. Should this occur, you may be required to re-register.

If you were not provided with a grace period or your grace period has expired, you will be forced to re-register.

![Sample Re-Registration Mandate](image)

Click **Re-register** to launch the Registration wizard.

If you need to re-register for a password-based account, follow the instructions under “Password Registration” on page 9.

If you need to re-register for a token-based account and you have been issued your token, follow the instructions under “Token Registration” on page 10.

If you can’t complete re-registration, click **Log Off Windows**. This could occur if you receive the prompt before you receive your token. The next time you boot up, you will receive the same re-registration mandate.

Default Password Aging

**Basics**

You may have set a Default Password and/or Session Default Passwords for encryption and/or decryption. If your Policy Administrator applied password aging requirements, your Default and/or Session Default Passwords have a minimum age and a maximum age.

**Warning**

When a Default or Session Default Password’s maximum age begins to approach, you will receive a warning message when you log on to Windows.

![Default Password Expiration Warning](image)
Expiration
If a Default or an active Session Default Password expires during your current Windows session, you will be notified.

If your Default Password or a Session Default Password has expired, you will be notified upon logging on to Windows.

You must use the User Client Console to change the password or you will not be able to use it for encryption; instead, you may be prompted to enter a password every time you try to encrypt a file, if you do not have another active default password.
3. User Client Console

Overview

Basics
The User Client Console is available once Windows has loaded and allows you to:

- View the other users that have registered to Symantec Endpoint Encryption on your machine.
- Find out which Symantec Endpoint Encryption products are installed on your machine and their version numbers.
- See which policies are being enforced by Removable Storage.

In addition, you may be able to:

- Add or change your Symantec Endpoint Encryption password.
- Add or change the token you use to authenticate to Symantec Endpoint Encryption.
- Set or change your Authenti-Check questions and answers.
- Set or modify your Default Password(s) and/or Default Certificate(s).
- Change your automatic encryption setting.

Launch
The User Client Console launches automatically when you complete the registration wizard, to encourage you to review your settings.

To launch the User Client Console, click Start, point to All Programs, point to Symantec Endpoint Encryption Client, and then click Symantec Endpoint Encryption Client. Alternatively, right-click the Symantec Endpoint Encryption icon in the Windows notification area and select Launch Symantec Endpoint Encryption User Client. One of four results will occur:

- The Logon panel appears (“Logon Panel” on page 17).
- The Home panel appears (“Home Panel” on page 21).
- You are prompted to register (“Registration Wizard” on page 6).
- You are advised that all user account slots have been taken and you cannot register. Contact your Client Administrator.

Single Sign-On
If Single Sign-On is enabled, when you click the close button on the User Client Console, you will be asked whether you want to log off of your Symantec Endpoint Encryption session. If you click Yes, the next time you launch the User Client Console, you will need to authenticate. If you click No, you will not have to log on to the User Client Console the next time you launch it in this Windows session.

Logon Panel

Basics
If your computer is set for automatic authentication, you should not need to log on to the User Client Console. Skip to “Home Panel” on page 21.
Otherwise, when the User Client Console launches, it prompts you for your credentials. Only the user currently logged on to Windows can log on to the User Client Console. For password authentication, continue to the next section. For token authentication, skip to “Token” on page 19. For logon assistance, skip to “Authentication Assistance” on page 20.

**Password**
If you have a Symantec Endpoint Encryption password, you can use it to log on to the User Client Console.

![User Client Console Logon, Password](image)

The **Authentication Method** drop-down list will only be displayed if you are allowed to authenticate with either a password or a token and you have defined both. To log on to the User Client Console with a password, ensure that **Password** is selected.

To log on to the User Client Console with a password, type your Symantec Endpoint Encryption password in the **Password** field, then click **Log On**.

If your password is not correct, the logon fails. Check your password and re-enter the information.

You may be forced to wait before you can log on. Logon delays protect against automated password-guessing attacks. The length of the delay will be shown as a countdown.

If your password is correct, you are given access to the User Client Console. Skip to “Home Panel” on page 21.
**Token**

If you registered with a token or you added a token to your account following registration, you can use it to log on to the User Client Console.

The **Authentication Method** drop-down list will only be displayed if you are allowed to authenticate with either a password or a token and you have defined both. Select **Token** from the **Authentication Method** drop-down list.

If your token is not already inserted, insert it now. For proper insertion of your token and for a description of token behavior when the token is being read, refer to Appendix B “Token Usage” on page 83. Make sure the token has been read before you proceed with authentication.

In the **PIN** field, type your PIN, then click **Log On**.

If you encounter token, certificate, or PIN errors during logon, please refer to Appendix C “User Client Console” on page 98 for possible causes and resolution.

If the **Select Certificate** dialog appears, continue reading, otherwise, skip to the next section.

Once you have successfully entered your PIN, if your token contains multiple valid certificates or no certificates, you may be asked to select a certificate.
Select your Symantec Endpoint Encryption certificate by clicking on the appropriate row in the Select Certificate dialog, then click OK.

If you don’t know which of the certificates listed are valid, or if no valid certificates are listed, contact your administrator. If you select a certificate that is not valid, you will receive an error message. Refer to Appendix C “User Client Console” on page 98 for possible causes and resolution.

**Authentication Assistance**

If your administrator has provided you with the Authenti-Check feature and you have defined your question-answer pair(s), the Authentication Assistance button will be available from the Logon panel. Click Authentication Assistance if you forgot or do not have the credentials associated with your account.

![Figure 3.4—User Client Console Logon, Authenti-Check](image)

Authenti-Check involves up to three question-answer pairs established either during registration or from the User Client Console.

In each box that appears beside a question, type the correct answer. The answers are not case-sensitive.

Once you have answered the questions, click Log On. One of the following will result:

- The Home panel will be displayed.
- You will be advised that your answers were incorrect.
- 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, you are returned to the Logon panel where the Account name and Password fields are unavailable. A message informs you that the number of allowed logon attempts has been exceeded and a running countdown displays how long you must wait before you can try again.
**Home Panel**

The User Client Console opens with the Home panel, an enabled navigation pane, and tasks that you may want to perform but have not yet completed, if any.

![Figure 3.5—User Client Console, Home](image)

From time to time, your Policy Administrator may push out new policies that require you to take action. You will be notified of your action items on the Home panel. If a panel is included in the action item, go to the panel listed by clicking its link, then update the information as specified on the Home panel. Each time you submit the updated information, you are returned to the Home panel and that action item is removed from the list.

Figure 3.5 shows action items that could appear. All of the possible action items, their meaning, and the action you need to take are described in the following table.

<table>
<thead>
<tr>
<th>Action Item</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please go to the <strong>Authenti-Check</strong> panel to update your Authenti-Check question/answer pairs.</td>
<td>Either the questions and/or their type (pre-defined, required, or optional) have changed, or Authenti-Check is being enabled for the first time.</td>
<td>From the navigation pane, click <strong>Authenti-Check</strong>. Refer to “Account Settings, Authenti-Check Panel” on page 30.</td>
</tr>
<tr>
<td>You may add a password to your account. To do this, please navigate to the <strong>Password</strong> panel and follow the instructions there.</td>
<td>You are allowed to authenticate with either a token or a password. You registered with a token but can add a password. Once you have defined both methods, you can use either one to authenticate to Symantec Endpoint Encryption.</td>
<td>From the navigation pane, click <strong>Password</strong>. Refer to “Account Settings, Password Panel” on page 26.</td>
</tr>
</tbody>
</table>
You may add a token to your account. To do this, please navigate to the Token panel and follow the instructions there.

You are allowed to authenticate with either a token or a password. You registered with a password but can add a token. Once you have defined both methods, you can use either one to authenticate to Symantec Endpoint Encryption.

From the navigation pane, click Token. Refer to “Account Settings, Token Panel” on page 28.

To specify one or more default certificates for Removable Storage, go to the Certificates panel.

You haven’t set any Default Certificates.

To set one or more Default Certificates, click Certificates in the navigation pane. Refer to “Removable Storage, Certificates Panel” on page 35.

To specify a Default Password and one or more Session Default Passwords for Removable Storage, please go to Default Passwords panel. You will be prompted for a password to protect each file you save to removable storage devices until you have created a Default Password or one or more Session Default Passwords.

You haven’t set any Default or Session Default Passwords.

To set a Default and/or Session Default Password(s), click Default Passwords in the navigation pane. Refer to “Removable Storage, Default Passwords Panel” on page 34.

Your Removable Storage default password has expired. To change it, go to the Default Passwords panel.

A password aging policy has been applied to your Default Password.

To set a Default Passwords, click Default Passwords in the navigation pane. Refer to “Removable Storage, Default Passwords Panel” on page 34.

Your Removable Storage session default password has expired. To change it, go to the Default Passwords panel.

A password aging policy has been applied to your Session Default Passwords.

To set one or more Session Default Passwords, click Default Passwords in the navigation pane. Refer to “Removable Storage, Default Passwords Panel” on page 34.

Session Default Passwords are deactivated at the end of each Windows session.

You will be forced to activate your Session Default Passwords when you begin a new Windows session.

To activate one or more Session Default Passwords, click Default Passwords in the navigation pane. Refer to “Removable Storage, Default Passwords Panel” on page 34.

Session Default Passwords are deleted at the end of each Windows session.

You will need to create your Session Default Passwords when you begin a new Windows session.

To set one or more Session Default Passwords, click Default Passwords in the navigation pane. Refer to “Removable Storage, Default Passwords Panel” on page 34.
Table 3.1—Home Panel Action Items (Continued)

<table>
<thead>
<tr>
<th>Action Item</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are one or more device encryption exemptions in place. When an exempted device is inserted into your computer, you will be presented with a pop-up message informing that the device is exempted from encryption and that files written to the device will not be encrypted.</td>
<td>Certain devices have been exempted from automatic encryption. If you have been provided with the ability to initiate encryption on demand, you won’t be able to do so on an exempted device.</td>
<td>The next time you log on, use your Windows password as your Symantec Endpoint Encryption password.</td>
</tr>
<tr>
<td>Your Symantec Endpoint Encryption password has been changed successfully to match your Windows password.</td>
<td>A Single Sign-On policy has been applied to your account. Removable Storage has synchronized your Symantec Endpoint Encryption password with your Windows password.</td>
<td></td>
</tr>
</tbody>
</table>

**Navigation**

**User Interface Elements**
The User Client Console is divided into several sections.

![Figure 3.6—User Client Console, User Interface Elements](image-url)
The sections are as follows:

- The banner displays the product logo, the name of the currently logged on user, and the user’s domain or local computer name.

- The navigation pane contains hyperlinks to all panels. A panel loads into the main pane when its link is clicked. The links are clustered under the following headings: Registered Users, Account Settings, Removable Storage, and an About link.

- 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.

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.

You can navigate the User Client Console using a mouse or keyboard.

**Mouse Navigation**

If you are using a mouse to navigate the User 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**

**Access Keys**

Use the keys listed in Table 3.2 to directly access User Client Console panels.

**Table 3.2—Access Keys**

<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>Account Settings</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>ALT+P</td>
</tr>
<tr>
<td>Token</td>
<td>ALT+K</td>
</tr>
<tr>
<td>Authenti-Check</td>
<td>ALT+A</td>
</tr>
<tr>
<td>Removable Storage</td>
<td></td>
</tr>
<tr>
<td>Removable Storage</td>
<td>ALT+R</td>
</tr>
<tr>
<td>Default Passwords</td>
<td>ALT+F</td>
</tr>
<tr>
<td>Certificates</td>
<td>ALT+T</td>
</tr>
<tr>
<td>User Choice</td>
<td>ALT+O</td>
</tr>
<tr>
<td>About</td>
<td>ALT+B</td>
</tr>
</tbody>
</table>

**TAB Key Access**

You can also use the TAB key to navigate the User Client Console.

- 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.
- To select a check box or activate a button, press the TAB key to place focus on the check box or button, then press ENTER or the SPACEBAR.

You may need to press TAB 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 Panel**

The Registered Users panel provides a view of all Symantec Endpoint Encryption registered user accounts on this computer.

From the navigation pane click *Registered Users*. The Registered Users panel appears, listing all current users.

![Figure 3.7—User Client Console, Registered Users](image)

The Registered Users panel can be useful for seeing who else has registered with Symantec Endpoint Encryption on your computer and how many more users can register.
Account Settings, Password Panel

Basics
You can use the Password panel to change your Symantec Endpoint Encryption password if Single Sign-On is not enabled. You can also use the Password panel to add a Symantec Endpoint Encryption password if you have your choice of authentication methods: password or token. Click Password from the navigation pane. The Password panel appears.

Single Sign-On Not Enabled
If Single Sign-On is not enabled and you need to add or change your Symantec Endpoint Encryption password, the New password and Confirm new password boxes will be displayed.

Define a password that you can remember, so that you don’t have to write it down. Longer passwords are more secure than short passwords. Include a variety of characters, including upper and lowercase letters mixed with numbers and special characters, if allowed. When you create a password, think of one that is hard to guess; for example, don’t use a commonly known fact, such as your spouse’s name, or a fact that can be easily researched, such as your mother’s maiden name.

If password management is enabled, the Password panel displays the required password length and the symbols that are allowed in your password, and any requirements for the number of symbols, uppercase letters, lowercase letters, and/or digits that your password must contain. Your panel will also describe any overall requirements, such as, “Your new password must be different than the last 10.”

Symbols allowed identifies which of the non-alphanumeric characters on your keyboard may be included in the password. Include at least displays the number of required symbols, uppercase letters, lowercase letters, and/or digits that your password must contain, if any.

In the New password field, enter your new Symantec Endpoint Encryption password.

In the Confirm new password field type your new password again.
Click **OK**.

- If your password meets the requirements, your password is updated and the Home panel (“Home Panel” on page 21) replaces the Password panel.

- If the password change is not allowed—for example, if not enough time has elapsed since you last changed your password—the fields and buttons become unavailable. An error message box will inform you of the nature of the problem. On the message box, click **OK** to dismiss the box. You can select another task from the navigation pane or click the User Client Console.

- If the password change is allowed but the password does not comply with the password requirements, then the requirement that the password does not satisfy is highlighted in red. Make the changes necessary to bring it into compliance, then click **OK** to resubmit the password.

At any time you may exit the panel by choosing another task from the navigation pane or clicking to quit the User Client Console. Your password will not be changed.

If you click **Cancel**, the fields are cleared and your password is not submitted.

**Single Sign-On Enabled**

If Single Sign-On is enabled and you have your choice of authentication methods, you can use the Password panel to add a Symantec Endpoint Encryption password to your account. This option is useful if you registered using a token, but have both a token and a password account in Windows, and want to be able to log on to Full Disk with either. To add a password, you must first log on to Windows using your password account. If you aren’t already logged on to Windows with your password account, the Password panel will prompt you to do so.

![Figure 3.9—User Client Console, Account Settings, Password, SSO Enabled](image)

To add a Symantec Endpoint Encryption password to your account, select the **Use my Windows password to create my Symantec Endpoint Encryption password account** check box. Then click **OK**. A confirmation message will be displayed.
**Account Settings, Token Panel**

**Basics**  
Use the Token panel to add or change the token that you use to authenticate to Symantec Endpoint Encryption. From the navigation pane, click *Token*. The Token panel appears.

**Token Change**  
If your administrator has provided you with a new token, you can use the Token panel to associate it with your new account.

![Figure 3.10—User Client Console, Account Settings, Token Panel with Existing Token](image)

The top section of the panel will display the token information currently associated with your Symantec Endpoint Encryption account.

To change this token, insert the new token. Type the PIN. Click **OK**.

Figure 3.10—User Client Console, Account Settings, Token Panel with Existing Token
**Token Addition**
If you have the option of authenticating with either a password or a token and do not yet have a token associated with your account, the Token panel will provide you with the opportunity of adding one.

![User Client Console, Account Settings, Token Panel without Existing Token](image)

Figure 3.11—User Client Console, Account Settings, Token Panel without Existing Token

To add a token, insert it. Type the PIN. Click **OK**.
Account Settings, Authenti-Check Panel

Use the Authenti-Check panel to modify the question-answer pairs that will allow you to gain access to the User Client Console if you are missing your token, PIN, or password. From the navigation pane, click Authenti-Check. The Authenti-Check panel appears.

![Authenti-Check panel](image)

Figure 3.12—User Client Console, Account Settings, Authenti-Check

Your Authenti-Check answers will not be displayed, once they have been stored, for security reasons.

Try to choose answers that other people cannot guess easily. Follow similar guidelines for your questions and answers as you would for your password. Create pairs that:

- Do not contain commonly known information,
- Are longer rather than shorter, and
- You can remember without writing down.

The following table provides examples of secure and less secure questions.

<table>
<thead>
<tr>
<th>Secure</th>
<th>Less Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who was your favorite teacher?</td>
<td>What is your social security number?</td>
</tr>
<tr>
<td>Who was your childhood hero?</td>
<td>Where were you born?</td>
</tr>
<tr>
<td>What is the street name where your favorite relative lived?</td>
<td>What is your mother’s maiden name?</td>
</tr>
</tbody>
</table>

When entering questions and answers, consider the following:

- Answers are visible when typed, so be sure no one is watching you type them. These answers are as important as your password.
Remember your answers. The answers are not case-sensitive.

Questions and answers marked required must be completed. Minimum and maximum character lengths are indicated in parentheses beside Questions and Answers. Even if a question or answer is marked optional, consider filling it in as it will increase the security of your data.

When you have entered all questions and answers, click OK to submit your information.

If your questions and answers are accepted, your information is updated. The Home panel (“Home Panel” on page 21) appears, replacing the Authenti-Check panel.

If your questions and answers are not accepted, the field that needs correcting turns red. Make your corrections. Click OK again.

If you click Cancel, your information is cleared and not submitted.

**Removable Storage Panel**

The Removable Storage panel will inform you of the policies in place on your machine. From the navigation pane click **Removable Storage**.

![Removable Storage Panel](image)

Figure 3.13—User Client Console, Removable Storage

Removable Storage is protecting your 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 data written to CD/DVD media,
- By automatically encrypting files per Symantec Data Loss Prevention for Endpoint, and/or
- By encrypting files written to a removable storage device on demand.
The Removable Storage panel will inform you which of these policies is in place on your machine.

Table 3.3—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>You cannot read from or write to removable storage devices from this computer.</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.</td>
<td>Once you have registered, you can read from but cannot write 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.</td>
<td>Once you have registered, you can read from and write 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>Unencrypted files stored on removable storage devices will be encrypted by Removable Storage as soon as they are accessed. You will be warned of this and given an option to view only, thereby preventing the encryption of unencrypted files (see “Pre-Existing Unencrypted Files” on page 39). Any file that you write to a removable storage device will 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>Any file that you write to a removable storage device will be encrypted by Removable Storage. You may be able to change this in the User Choice panel (see “User Choice Panel” on page 37).</td>
<td>Encryption Policy: Encrypt New</td>
</tr>
<tr>
<td>New files written to these devices are not encrypted.</td>
<td>Removable storage device files will not be encrypted by Removable Storage. You may be able to change this in the User Choice panel (see “User Choice Panel” on page 37).</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>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 the devices.</td>
<td>You 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>
The following groups of file types are exempt from encryption: Audio | Video | Image

Removable Storage will not encrypt files belonging to the itemized group(s) when enforcing an encrypt all, encrypt new, or CD/DVD only encryption policy. See Appendix A “Multimedia File Types Excluded” on page 78 for the file types that belong to each group.

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.

If you are prompted for a password during file encryption on a removable device, you can choose to have Removable Storage remember that password as a default password for that device only, as long as the device is inserted and you are logged on to Windows.

<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 exempt from encryption: Audio</td>
<td>Removable Storage will not encrypt files belonging to the itemized group(s) when enforcing an encrypt all, encrypt new, or CD/DVD only encryption policy. See Appendix A “Multimedia File Types Excluded” on page 78 for the file types that belong to each group.</td>
<td>Default Passwords Policy: Allow device session default passwords</td>
</tr>
<tr>
<td>Video</td>
<td>Image</td>
<td></td>
</tr>
<tr>
<td>If you are prompted for a password during file encryption on a removable device, you can choose to have Removable Storage remember that password as a default password for that device only, as long as the device is inserted and you are logged on to Windows.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Removable Storage, Default Passwords Panel

If your computer has been configured to encrypt files automatically, you may want to set a Default Password and/or up to two Session Default Passwords. Click Default Passwords from the navigation pane.

To set and/or activate a Default Password, select the Set a default password check box. To set a new Default Password or change an existing Default Password, type the Default Password in the Password box and again in the Confirm password box. To deactivate a Default Password, deselect the Set a default password check box. The optional Memo field lets you provide a reminder of the password value you have chosen.

To set and/or activate a Session Default Password, select a Set a session default password check box. To set a new Session Default Password or change an existing Session Default Password, type the Default Password in the Password box and again in the Confirm password box. To deactivate a Session Default Password, deselect the Set a session default password check box. The optional Memo field lets you provide a reminder of the password value you have chosen. Depending on your organization’s policy, you may find that your Session Default Passwords get deactivated or deleted at the end of a Windows session. Refer to the Home panel to discover if such a policy is in effect.

Your files will be encrypted using the Default Password and/or Session Default Password(s). In addition, if an active Default Password and/or Session Default Password matches one of the passwords that a file was encrypted under, it will be decrypted automatically.
When setting a password, try to pick something that you can remember without having to write it down. Avoid words that can be easily guessed by people who know you, such as the name of your dog, or your mother's maiden name. If possible, avoid words that can be found in the dictionary.

Keep your Default Password and/or Session Default Passwords secure so that you will not have to change it unnecessarily. Here are the reasons you may have to change your Default Password or Session Default Password:

- You believe that it has been compromised.
- Your administrator has required you to do so at a designated interval.

Keep in mind that when you change a Default or Session Default Password, the new password will be used to encrypt files from that point forward. In order to open files that were encrypted under the previous password, you will need to remember the previous password. For this reason, you may want to copy all files off of your removable storage device after changing a Default Password or Session Default Password. Then copy them back on to the device. That way they will be encrypted with the new Default or Session Default Password.

If you cannot remember a password associated with a file, contact your Client Administrator.

Once you have entered and confirmed your Default or Session Default Password, click OK. A confirmation message will be displayed. If password aging is enabled, you will see the aging requirement in the success confirmation.

**Removable Storage, Certificates Panel**

The Certificates panel allows you to view and manage your Default Certificates. To open the panel, click *Certificates* from the navigation pane.

![Figure 3.15—User Client Console, Removable Storage, Certificates](image)

To add a certificate, click *Add New Certificate*. The *Select Default Certificates* window appears.
The window is populated with the valid certificates that Removable Storage has found in the local certificate store. You can filter the list by using the Show Certificates Belonging To option buttons. The View Details button provides additional information about a highlighted certificate.

Once you have selected the check box of the certificate you want to add, click OK. The certificate appears on the Certificates panel. You can add up to ten Default Certificates.

To remove a certificate, on the Certificates panel select the check box next to one or more certificates. The Remove Selected Certificates button becomes enabled. Click the button.

Removable Storage will no longer have the removed Default Certificate(s) available when it attempts to decrypt files. As a result, you may be prompted to provide the removed Default Certificate(s).

If the Default Certificate(s) that you have removed have been replaced with one or more new Default Certificates, you should copy all of the files off of your removable storage device and then copy them back to the removable storage device. This will ensure that they are encrypted under the new Default Certificate(s).
User Choice Panel

The User Choice panel allows you to change your default automatic encryption setting. If your organization’s policy does not allow you to choose your automatic encryption default, the User Choice panel will be unavailable. To open the panel, click User Choice from the navigation pane.

![User Choice Panel Image]

Figure 3.17—User Client Console, Removable Storage, User Choice Panel

The initial selection is set by your organization’s administrator. Select **Encrypt new files written to removable media** to ensure that new files, by default, will be encrypted when written to removable media. Select **Do not encrypt new files written to removable media** to ensure that by default, files will not be encrypted when written to removable media. You can change the default at any time, and you can override the default for an individual file using a right-click menu command, if your organization’s policy allows that option.

If multimedia files have been exempted from encryption, they are not encrypted even if you choose **Encrypt new files written to removable media** as your default choice. Refer to the Removable Storage panel to discover if multimedia files have been exempted.

If devices have been exempted from encryption, files written to the exempted devices will not be encrypted even if you choose **Encrypt new files written to removable media** as your default choice. Refer to the Home panel to discover if such a policy is in place.
**About Panel**

Use the User Client Console to find out which version of Framework and Removable Storage you are running.

From the navigation pane, click *About*. The About panel appears.

![Image of User Client Console, About](image)

The build number associated with a given version number is accessible as a Tooltip. Hover your mouse over the version number. The build number displays. 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 Encryption/Decryption

Overview

If files written to removable storage devices are being encrypted automatically, your administrator has configured your computer to use a password, a certificate, or both.

Each time Removable Storage encrypts a file, it will need to know which password(s) and/or certificate(s) to use. Once the file is encrypted under the specified password(s)/certificate(s), the specified password(s)/certificate(s) will need to be provided before the file can be decrypted.

This chapter discusses the following:

- Pre-existing unencrypted files under an encrypt all policy (“Pre-Existing Unencrypted Files” on page 39),
- Defining passwords and/or certificates on a per file basis (“Encryption Prompts” on page 40, “Decryption Prompts” on page 44),
- Encrypting and decrypting files using right-click menu options (“On Demand Encryption” on page 46), and
- Renaming of duplicate files (“Two Files With Same Name” on page 47).

Pre-Existing Unencrypted Files

Your administrator may have configured your computer so that all previously unencrypted files on removable devices are encrypted when they are accessed. If this setting is enabled, a message displays when you insert removable media for the first time in your Windows session, whether or not the media contains any pre-existing unencrypted files. You will not see the message, however, if your device is blank, if it is a CD or DVD, or if it is a device that has been excluded from encryption by your administrator.

Figure 4.1—Plaintext File Message
If you click **Continue**, it is very likely that any unencrypted files stored on removable media (except for CDs and DVDs) will be encrypted. Accessing the file includes moving your mouse pointer over a file, selecting a file, opening a file, setting the folder view to **Details**, having AutoPlay enabled, or having an anti-virus program installed.

If your administrator has exempted multimedia file types, and/or certain devices from automatic encryption, files of those multimedia type(s), or on the exempted device(s) will not be encrypted when accessed. The Removable Storage panel in the Client Console lists any multimedia file types and/or removable storage devices that are excluded from encryption (“Removable Storage Panel” on page 31).

If you do not want existing files on the removable media to be encrypted, click **Limited Access** or remove the device. If you select **Limited Access**, you will be able to view the list of files stored on the removable device, but will not be able to open any files.

To modify your selection, remove and reinsert the removable media. The message will display again and you can select **Continue** or **Limited Access**, as desired.

If your administrator has exempted devices from encryption, a message is displayed when you insert removable media of that type for the first time in your Windows session.

![Symantec Endpoint Encryption Removable Storage](image)

**Figure 4.2—Exempted Devices Message**

**Encryption Prompts**

**Basics**
If your computer is configured to encrypt files automatically and you haven’t set a Default Password, Session Default Passwords, and/or Default Certificate(s), you will be prompted each time you attempt to write a file to removable media. The prompt will vary according to the encryption method set by your administrator.

If your administrator has configured your computer to use passwords to encrypt files, a prompt similar to the following will be displayed.
It will be necessary to remember the password that you enter at the prompt in order to decrypt the file later on. When setting a password, try to pick something that you can remember without having to write it down. Avoid words that can be guessed easily by people who know you, such as the name of your dog, or your mother’s maiden name. If possible, avoid words that can be found in the dictionary.

Depending on how your administrator has configured your computer, the password that you enter will need to meet certain requirements.

- If your administrator has set certain password requirements, they will be noted in any error message that displays. The requirements are also listed in the User Client Console Password panels (“Account Settings, Password Panel” on page 26 and “Removable Storage, Default Passwords Panel” on page 34).
- If your administrator did not configure any password requirements, you must enter a minimum of eight characters.

The **Remember this password while this device is connected** check box will be displayed if you are allowed to set this password as a default password for this device. Select the **Remember this password while this device is connected** check box if you would like Removable Storage to use this password to encrypt all files written to this device as long as it remains connected or until you log off of Windows.

💡 Reformatting the device also clears the password.

Type the password to be used to encrypt and decrypt the file in the **Enter Password** field. Confirm your entry by entering the password again in the **Confirm Password** field. Click **OK**.
**Certificate(s)**

If your administrator has configured your computer to use certificates to encrypt files, a prompt similar to the following will be displayed.

![Encryption Certificate Prompt](image)

You can select up to ten certificates to be used to encrypt the file. You, or your fellow Removable Storage users, will need to provide at least one of the specified certificates before the file can be decrypted.

By default, the **Myself** option will be selected, ensuring that only certificates that reside within the **Personal** certificate store are listed in the **Select certificates** box. This includes certificates that reside on a token that you have inserted. If you don’t see the certificate(s) from your token in the box, click **Refresh**.

Click **Other People** to display only certificates that reside in the **Other People** certificate store. This would only be useful to you if you wanted to encrypt a file using a certificate containing someone else’s public key. Then only that person would be able to decrypt the file, because they would be the only one with the private key.

To show both certificates that reside in the **Personal** and in the **Other People** certificate store, click **All**.

The **View Details** button can be used to find out more about the certificate highlighted in the **Select certificates** box.

Once you have selected the certificate(s) to be used to encrypt the file, click **OK**.
Password/Certificate(s)
If your administrator has configured your computer to use passwords and/or certificates to encrypt files, a prompt similar to the following will be displayed.

![Encryption Password/Certificate Prompt](image)

Figure 4.5—Encryption Password/Certificate Prompt

You can enter a password, select one or more certificates, or do both. In Figure 4.5, a password has been specified and two certificates have been selected. Any one of these can be used to decrypt the file.

Depending on how your administrator has configured your computer, the password that you enter will need to meet certain requirements.

- If your administrator has set certain password requirements, they will be noted in any error message that displays. The requirements are also listed in the User Client Console password panels ("Account Settings, Password Panel" on page 26 and "Removable Storage, Default Passwords Panel" on page 34).

- If your administrator did not configure any password requirements, you must enter a minimum of eight characters.

The **Remember this password while this device is connected** check box will be displayed if you are allowed to set a Device Session Default Password. Select the **Remember this password while this device is connected** check box if you would like Removable Storage to use this password to encrypt all files written to this device as long as it remains connected or until you log off of Windows. If you are encrypting with one or more certificates as well as with a password—and you have selected the **Remember this password while this device is connected** check box—the file that triggered this prompt will be encrypted with both the password and the certificate(s). You will no longer receive a prompt for subsequent file encryption on this device, and all further encryption will be to the default password only. If you would like to encrypt more files using certificates, remove the device then reinsert it; you will be prompted each time for a password and/or certificates.

Type the password to be used to encrypt and decrypt the file in the **Enter Password** field. Confirm your entry by entering the password again in the **Confirm Password** field.
The certificates located in your local certificate store will be listed in the Select certificates box. If you want to use a certificate that is stored on a token, insert your token. Once it is recognized by your token reader and token software, the certificates on the token will be available from within your local certificate store and will be listed in the dialog. If they do not appear, click Refresh.

The list will be filtered to include only those certificates issued to yourself, as the Myself option button will be selected by default. To expand the range of displayed certificates, you can select either the Other People or the All option buttons.

The View Details button can be used to find out more about a certificate highlighted in the Select certificates box. Once you are satisfied with your selections and/or entries, click OK.

Decryption Prompts

Basics
Removable Storage will try to decrypt files using your Default Password, Default Certificate, Device Session Default Password, as well as any credentials you’ve already provided during the Windows session. If none of these credentials match the credentials the file was encrypted under, you will be prompted either to enter the password it was encrypted under or to provide the certificate that was used to encrypt it.

Password
If the file was encrypted under a password, you will be prompted to enter the password it was encrypted under. This prompt will occur at the time that Windows attempts to open the file.

![Figure 4.6—Decryption Password Prompt](image)

Enter the password that the file was encrypted under and click OK. If you provide the wrong password too many times, you may be forced to wait one minute before trying again. The number of attempts you have before the one-minute delay is effected is shown beside Attempts remaining.

If you click Cancel, you will not be able to open the file later during the device session. To open such a file later, remove and reinsert the removable storage device. This time, when Removable Storage requests a password, enter the necessary password.

Certificate(s)
If the file was encrypted under one or more certificates and the certificates it was encrypted under cannot be found in your local certificate store, you will be prompted to insert a token that contains the necessary certificate. This prompt will occur at the time that Windows attempts to open the file.
If the necessary certificate resides on a token, insert the token and click **Retry**.

Depending on your token software, after the software reads your token, you may be prompted to enter your PIN.

If you are prompted to enter your PIN, do so and click **OK**. Your local certificate store will be populated with the certificates that reside on the token and as long as Removable Storage locates the necessary certificate in your local certificate store, decryption will succeed without further messages.

**Password/Certificate(s)**

If the file was encrypted under both a password and one or more certificates, and none of the certificates that the file was encrypted under can be found in your local certificate store, you will be prompted to enter either the password or select one of the certificates it was encrypted under.
To enter a password, accept the default Enter Password option button selection and type the password into the text field and click OK. If you provide the wrong password too many times, you may be forced to wait one minute before trying again. The number of password attempts you have before the one-minute delay is instantiated is shown beside Attempts remaining.

To use a certificate, select the Have certificate on a smart card option button, insert the token that contains the appropriate certificate, then click OK. The token software will read the token and prompt you for your PIN. Once you authenticate to the token, the decryption will proceed.

If you click Cancel, you will not be able to open the file during the device session. To open such a file later, remove and reinsert the removable storage device. This time, when Removable Storage requests a password or certificate, enter or select the necessary password or certificate.

**On Demand Encryption**

**Basics**
Your administrator may have configured your computer to allow you to selectively encrypt or decrypt individual files, groups of files, folders, or groups of folders saved on removable storage devices. An administrator can configure the encrypt and decrypt features separately—for example you may be able to encrypt files on demand but not decrypt them, or vice versa.

**Right-Click File Encryption**
On the removable storage device, browse to the location of the file(s) you want to encrypt. You can select multiple individual files, or you can select one or more folders. Right-click the selected file(s), point to Symantec, and select Encrypt.

If you have an active Default Password, Session Default Passwords, and/or Default Certificate(s), all of them are used to encrypt the file(s). Any one of them can be used to decrypt the resulting encrypted files. If no Default Passwords or Certificates have been set, you will be prompted to enter a password or provide a certificate (“Encryption Prompts” on page 40).

The right-click file encryption option has several restrictions:
- If the file you select is already encrypted, the Encrypt menu option is not available.
- The Encrypt menu option cannot be used with files or folders burned to CD/DVD.
- The Encrypt menu option cannot be used if the removable storage device is an exempted device.
- The Encrypt menu option can be used to select and encrypt multimedia files even though those file types may be excluded from automatic encryption.

When selecting a group of files, a folder, or a group of folders to be encrypted, the following conditions apply:
- If you select a group of files or a folder, and some of the files in the group or folder are already encrypted, you can use the Encrypt menu option. The files that are already encrypted are skipped, while the remaining files are encrypted.
- If you select a group of folders, and all the files within a selected folder are encrypted, that folder is skipped. The unencrypted files in the remaining folders are encrypted.

**Right-Click File Decryption**
On the removable storage device, browse to the location of the file(s) you want to decrypt. You can select multiple individual files, or you can select one or more folders. Right click the selected file(s), point to Symantec, and select Decrypt.
If any one of the Default Passwords or certificates used to encrypt the file are available to Removable Storage, the file is decrypted without a further prompt. If none of the passwords or certificates are available you will be prompted to enter a password or provide a certificate (“Decryption Prompts” on page 44).

The right-click file encryption option has several restrictions:

- If the file you select is already decrypted, the **Decrypt** menu option is not available.
- The **Decrypt** menu option cannot be used with files or folders burned to CD/DVD.

When selecting a group of files, a folder, or a group of folders to be encrypted, the following conditions apply:

- If you select a group of files or a folder, and some of the files in the group or folder are already decrypted, you can use the **Decrypt** menu option. The files that are already decrypted are skipped, while the remaining files are decrypted.
- If you select a group of folders, and all the files within a selected folder are decrypted, that folder is skipped. The encrypted files in the remaining folders are decrypted.

**Two Files With Same Name**

If your computer is configured to encrypt files automatically, certain sequences of events could cause you to end up with two files of the same name on your device: one encrypted and the other unencrypted. These files will be named as follows:

- `file name.file extension`
- `file name.file extension.xml`

For example, My Spreadsheet.xls and My Spreadsheet.xls.xml. The file bearing the XML extension is the encrypted file. You will be able to observe these duplicate files only while working at a computer not protected by Removable Storage.

This could occur through circumstances such as the following:

- While at a computer not protected by Removable Storage, you used the Removable Storage Access Utility to encrypt a file. You saved the encrypted file to your device with same name as a file already on the device and selected the **Preserve original unencrypted file** check box. The operating system did not catch this because the Removable Storage Access Utility appended an XML to the end of the file name to signify that the file is encrypted.
- You transported your removable storage device from a computer protected by Removable Storage to a computer not protected by Removable Storage. While at the computer not protected by Removable Storage, you saved a file to the device bearing the same name as a file already on the device. The operating system did not catch this because the file already on the device bore an XML extension, because it was encrypted.

Should this situation occur, Removable Storage will resolve the issue by renaming the unencrypted file. The renamed file will have the exact same number of characters in its file name, according to the convention below:

- `file na~n.file extension`
- `file name.file extension`
Most commonly, the n character will be a zero. However, if a file with the same name is already on the device, the n will increment.

For example, the files My Spreadsheet.xls and My Spreadsheet.xls.xml will become My Spreadsheet-0.xls and My Spreadsheet.xls.

The renaming will occur as soon as the operating system attempts to access the file. Most often, this will occur as soon as you insert your device.
5. Self-Extracting Executables

Overview
Your administrator may have configured your computer to allow you to create encrypted self-extracting executables for secure transport. Such files can be decrypted from computers not protected by Removable Storage and by recipients not in possession of the Removable Storage Access Utility.

Do not attempt to create a self-extracting executable larger than 4 GB.

Self-Extracting Archive Encryption

Save Archive
Browse to the location of the file(s) that you want to encrypt. A single file or multiple files can be encrypted to a self-extracting archive. Right-click the selected file(s), point to Symantec, and select Encrypt to self-extracting archive.

The Removable Storage Self-Extracting Archive dialog appears.

Figure 5.1—Self-Extracting Archive, Encryption

Figure 5.1 shows an example of the dialog for a user whose Removable Storage administrator allows both passwords and certificates to be used for encryption.
The dialog contains the same fields regardless of your encryption method; however, not all check boxes may be available. Check box enablement is described in Table 5.1.

**Table 5.1—Removable Storage Self-Extracting Archive Dialog Information**

<table>
<thead>
<tr>
<th>Encryption Method</th>
<th>Enabled Check Box</th>
<th>If You Select This Check Box</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password only</td>
<td>Use Removable Storage default password (conditional)</td>
<td>You apply your Default Password—that you have already set—to encrypt this archive. This option will only use the Default Password—not Session Default Password(s).</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>You manually define a password to encrypt this archive. The check box becomes disabled if you select the Use Removable Storage default password check box.</td>
</tr>
<tr>
<td>Certificates only</td>
<td>Certificates</td>
<td>The certificates in your local certificate store appear in the Certificates box. You select one or more of those certificates to encrypt this archive.</td>
</tr>
<tr>
<td>Passwords and/or Certificates</td>
<td>Use Removable Storage default password (conditional)</td>
<td>You apply your Default Password—that you have already set—to encrypt this archive. Note that Session Default Passwords cannot be used here.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>You manually define a password to encrypt this archive. The check box becomes disabled if you select the Use Removable Storage default password check box.</td>
</tr>
<tr>
<td></td>
<td>Certificates</td>
<td>The certificates in your local certificate store appear in the Certificates box. You select one or more of those certificates to encrypt this archive.</td>
</tr>
</tbody>
</table>

**File Name and Location Identification**

Regardless of your encryption method, follow the general instructions below for naming and identifying a location for the archive:

- In the **Archive Name** field, type a name for the self-extracting executable file. Alternatively, use the default **Archive Name** that is displayed, which consists of the system time and date, such as, “115408192008.exe.”
- Type the desired destination of the self-extracting executable in the **Encrypt to** field, or browse to the appropriate folder in the **Folders/Drives** box.
- To create a new folder or subfolder, select an existing folder then click the **New folder** button. The **Create Folder** dialog appears. In the **New folder** field, type the name of the new folder and click **OK**. Your folder is created and you are returned to the **Removable Storage Self-Extracting Archive** dialog.
- If you have already saved a self-extracting executable of the same name to this location and want to replace it with this one, select the **Overwrite existing files** check box.

**Encryption**

Follow the instructions below that are specific to your encryption method.

For the password-only encryption method:

- If you have set a Default Password, the **Use Removable Storage default password** check box is enabled. Select this check box to use your Default Password to encrypt this file.
If the **Use Removable Storage default password** is not enabled or selected, the **Password** check box will be enabled. Select this check box to encrypt the file under a password that you will specify manually. Type and confirm a password in the **Password** and **Confirm** fields. If your administrator has set certain password requirements and your password does not meet them, an error message will be displayed that states the requirements. The requirements are also listed in the User Client Console password panels (“Account Settings, Password Panel” on page 26 and “Removable Storage, Default Passwords Panel” on page 34).

Click **Encrypt**.

For the certificates-only encryption method:

- Select the **Certificates** check box to encrypt the file under one or more (up to 10) certificates. The certificates in your local certificate store appear in the **Certificates** box.

  ![Certificate Icon]

  If no certificates exist in your local certificate store, you will need to insert your token and authenticate with your PIN. The token software reads your certificates into your local certificate store.

- Click each check box under the **Select** column for the certificate or certificates that you would like to use. Click **Details** for any selected certificate to see specifics.

- Click **Encrypt**.

  For the password and/or certificates encryption method, follow the instructions for both password and certificate encryption above in this section.

  A message confirms that the archive has been encrypted and saved to the location you specified.

**Attach Archive**

Browse to the location of the file(s) that you want to encrypt and send by email. Right-click the selected file(s), point to **Symantec**, and select **Encrypt, rename and email**. The **Encrypt, Rename, and email** dialog appears.

![Encrypt, Rename, and email](image)

**Figure 5.2—Self-Extracting Archive, Encrypt, Rename, and Email**
Figure 5.2 shows an example of the dialog for a user whose Removable Storage administrator allows both passwords and certificates to be used for encryption.

The dialog contains the same fields regardless of your encryption method; however, not all check boxes may be available. Check box enablement is described in Table 5.2.

Table 5.2—Encrypt, Rename, and Email Dialog Information

<table>
<thead>
<tr>
<th>Encryption Method</th>
<th>Enabled Check Box</th>
<th>If You Select This Check Box</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password only</td>
<td>Use Removable Storage default password (conditional)</td>
<td>You apply your Default Password—that you have already set—to encrypt this archive. This option will only use the Default Password—not Session Default Password(s).</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>You manually define a password to encrypt this archive. The check box becomes disabled if you select the Use Removable Storage default password check box.</td>
</tr>
<tr>
<td>Certificates only</td>
<td>Certificates</td>
<td>The certificates in your local certificate store appear in the Certificates box. You select one or more of those certificates to encrypt this archive.</td>
</tr>
<tr>
<td>Passwords and/or Certificates</td>
<td>Use Removable Storage default password (conditional)</td>
<td>You apply your Default Password—that you have already set—to encrypt this archive.</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>You manually define a password to encrypt this archive. The check box becomes disabled if you select the Use Removable Storage default password check box.</td>
</tr>
<tr>
<td></td>
<td>Certificates</td>
<td>The certificates in your local certificate store appear in the Certificates box. You select one or more of those certificates to encrypt this archive.</td>
</tr>
</tbody>
</table>

**File Name**

The **Archive Name** field displays a default value of the system time and date with “.rse” appended as a file extension, such as “115408192008.rse.” You can change the archive name, but leave the extension unchanged. Most firewalls block files with an EXE extension. The RSE extension is designed to prevent the attached file from being stripped by the firewall.

**Encryption**

Follow the instructions below that are specific to your encryption method.

For the password-only encryption method:

- If you have set a Default Password, the **Use Removable Storage default password** check box is enabled. Select this check box to use your Default Password to encrypt this file.

- If the **Use Removable Storage default password** is not enabled or selected, the **Password** check box will be enabled. Select this check box to encrypt the file under a password that you will specify manually. Type and confirm a password in the **Password** and **Confirm** fields. If your administrator has set certain password requirements and your password does not meet them, an error message will be displayed that states the requirements. The requirements are also listed in the User Client Console password panels (“Account Settings, Password Panel” on page 26 and “Removable Storage, Default Passwords Panel” on page 34).
Click email.

For the certificates-only encryption method:

Select the Certificates check box to encrypt the file under one or more (up to 10) certificates. The certificates in your local certificate store appear in the Certificates box.

If no certificates exist in your local certificate store, you will need to insert your token and authenticate with your PIN. The token software reads your certificates into your local certificate store.

Click each check box under the Select column for the certificate or certificates that you would like to use. Click Details for any selected certificate to see specifics.

Click email.

For the password and/or certificates encryption method, follow the instructions for both password and certificate encryption above in this section.

Send

Your default email application opens and automatically creates an email with the encrypted self-extracting archive file attached.

Complete the email recipients and message text as needed and send the email. To ensure the security of the encrypted data, it is recommended that you communicate the password through another channel, such as in person or by phone.

Modify Archive

Basics

An archive can be modified by you or by a recipient if all of the following conditions are met:

- The computer is protected by Removable Storage.
- The person modifying the archive is a registered user.
- Decryption credentials are available or provided. Only one of the credentials used to encrypt the archive is required to open the archive and to delete files; all of the credentials are required to add files.

File Launch

To modify the contents of a self-extracting executable, double-click the archive.

Decryption Prompt: Password

If the archive was encrypted with the Default Password that was set on this computer, no password prompt appears. Proceed directly to “Package Modifier Open” on page 55.
If the archive was encrypted with another password, the **Symantec Endpoint Encryption Self-Extractor Password** dialog appears.

![Image](image1.png)

**Figure 5.3—Self-Extracting Archive, Decryption, Password Prompt**

Type the password with which this archive was encrypted in the **Password** field, then click **OK**. If the password is correct, proceed to “Package Modifier Open” on page 55.

If the password is not correct, type the correct password and click **OK** again. If you are prompted for a password but enter the wrong password too many times (that is, you exceed the number of **password attempts remaining** displayed on the dialog), you may be forced to wait one minute before trying again.

**Decryption Prompt: Certificates Only**

For archives that were encrypted using certificates only, if the required certificate(s) is already available on the computer, no decryption prompt appears. Proceed to “Package Modifier Open” on page 55.

If the required certificate is not available on the computer, this error message appears:

![Image](image2.png)

**Figure 5.4—Self-Extracting Archive, Decryption, Certificate Not Available**

If you insert the smart card then click **Retry**, the token software prompts you for your PIN. Once you authenticate, the certificates are read into the local certificate store, satisfying the decryption credential requirement. Proceed to “Package Modifier Open” on page 55.

If you click **Cancel** instead of **Retry**, access to the archive is denied.

**Password and Certificates: Certificates Available**

If the archive was encrypted using a password and one or more certificates—and at least one of those certificates is already available on the computer—no decryption prompt occurs. Proceed to “Package Modifier Open” on page 55.
Password and Certificates: Certificates Not Available

If the archive was encrypted using both a password and one or more certificates—and none of the certificates is available yet on the computer—the decryption prompt appears for either credential option.

You have the option of providing a password or a certificate. Do one of the following:

- Select the Password option and type the password with which the archive was encrypted. Click OK.
- Select the Have certificate on a smart card option. Insert your token then click OK. The system recognizes the card and prompts you for your PIN. Enter your PIN and click OK on the PIN prompt dialog.

Proceed to “Package Modifier Open” on page 55.

Package Modifier Open

Once credentials are verified, the Removable Storage Package Modifier dialog opens.
Once the archive is open, files or folders can be extracted (decrypted) or deleted. Files can also be added, once all credentials are available.

To navigate within the archive, select a folder then right click and select **Open Folder**. The contents of that folder are displayed. To go up one level, click the up arrow.

**Add Files**

To add one or more files to the existing archive, from the **Removable Storage Package Modifier** dialog, click the **Add Files** button, or from the **File** menu click right and select the **Add Files** option.

If certificates were used to encrypt the archive, those certificates must be available on the computer in the local certificate store or the add function is denied. If the certificates are not available, insert your token and authenticate with the PIN if prompted. The certificates are now available to the local certificate store; try again.

The **Add Files and Folders** dialog appears.

![Add Files and Folders](image)

**Figure 5.7—Self-Extracting Archive, Add Files**

Select the file(s) to add and click **Add**.

A message confirms that the file(s) is encrypted immediately and added to the archive. The **Removable Storage Package Modifier** dialog reappears; the new file(s) is included in the file list.

**Extract Files**

To extract one or more files, from the **Removable Storage Package Modifier** dialog (Figure 5.6), select one or more files. The file(s) can be extracted in one of three ways:

- Click the **Extract To** button, or
- From the **File** menu, right click and select the **Extract To** option, or
- Right click and select **Extract To**.
The Removable Storage Extractor dialog appears.

![Figure 5.8—Self-Extracting Archive, Extractor](image)

Type the location where you want to save the decrypted file(s) in the Extract To field. Alternatively, browse to the location in the Folders/Drives pane.

To create a new folder or subfolder, select an existing folder then click the New Folder button. At the Create Folder dialog, type the name for the new folder and click OK. The new folder is created in the location specified.

If the file has already been extracted to this location and you want to replace the previously decrypted file(s) with a more recent version, select the Overwrite existing files check box. The files will be overwritten without warning. If you do not select the Overwrite existing files check box and the files already exist in the specified location, you will be warned that the files exist and given a chance to confirm or deny that you would like to continue with the action.

If an error occurs during extraction, a message appears for each affected file.

If the action is successful, a message confirms the extraction. The file(s) are saved to the specified location.

Clicking Close or clicking the close button dismisses the extractor.

Delete Files
To delete one or more files from the archive, from the Removable Storage Package Modifier dialog select one or more files, then:

- From the File menu select the Delete From List option, or
- Right click and select Delete Selected Items, or
- Click the Delete button.

You are prompted to confirm that you really want to delete the file(s).

Self-Extracting Archive Decryption

Renaming Emailed Files
Once the self-extracting executable has been transported to a computer not protected by Removable Storage, the recipient must first ensure that the executable bears the correct EXE extension. If the file was emailed, it may need to be renamed. On a computer that is not protected by Removable Storage, decryption always happens.
**File Launch**
Once the file bears the necessary EXE extension, the recipient double-clicks or otherwise attempts to launch the file.

**Decryption Prompts**

*Password*
If the archive was encrypted using a password only, the **Removable Storage Extractor** dialog appears, with a password prompt.

![Removable Storage Extractor](image)

Figure 5.9—Self-Extracting Archive, Decryption, Password Prompt

The recipient types the location where they want to save the decrypted file(s) in the **Extract to** field. Alternatively, they can browse to the location in the **Folders/Drives** pane.

To create a new folder or subfolder, the recipient selects an existing folder then clicks the **New Folder** button. At the **Create Folder** dialog, the recipient types the name for the new folder and click **OK**. The new folder is created in the specified location.

If the recipient has already decrypted the file in this location and wants to replace the previously decrypted file(s) with a more recent version, they select the **Overwrite existing files** check box. The files will be overwritten without warning. If the recipient does not select the **Overwrite existing files** check box and the files already exist in the specified location, the recipient will be warned that the files exist and given a chance to confirm or deny that they would like to continue with the action.

The recipient types the password in the **Password** field, then clicks **Extract**. If the wrong password is provided too many times, the recipient may be forced to wait one minute before trying again.

If an error occurs during extraction, a message appears for each file affected.

If extraction is successful, a message confirms the extraction. The decrypted file(s) is saved to the specified location.
For archives that were encrypted using certificates only, if the required certificate is not available on the computer, this error message appears:

![Certificate Not Available](image)

Figure 5.10—Self-Extracting Archive, Decryption, Certificate Not Available

The recipient inserts their smart card then clicks **Retry**. The token software prompts them for their PIN. Once they authenticate, the certificates are read into the local certificate store, satisfying the decryption credential requirement. If the required certificate(s) is available on the computer already, no decryption prompt appears.

The **Removable Storage Extractor** dialog (Figure 5.11) launches.

![Removable Storage Extractor](image)

Figure 5.11—Self-Extracting Archive, Decryption, Certificate(s) Prompt

To extract the archive:

- The recipient types the location where they want to save the decrypted file(s) in the **Extract to** field. Alternatively, they can browse to the location in the **Folders/Drives** pane.

- To create a new folder or subfolder, the recipient selects an existing folder then clicks the **New Folder** button. At the **Create Folder** dialog, the recipient types the name for the new folder and click **OK**. The new folder is created in the specified location.
If the recipient has already decrypted the file in this location and wants to replace the previously decrypted file(s) with a more recent version, they select the **Overwrite existing files** check box. The files will be overwritten without warning. If the recipient does not select the **Overwrite existing files** check box and the files already exist in the specified location, the recipient will be warned that the files exist and given a chance to confirm or deny that they would like to continue with the action.

If an error occurs during extraction, a message appears for each file affected.

If extraction is successful, a message confirms the extraction. The decrypted file(s) is saved to the specified location.

**Password and Certificates: Certificates Available**

If the archive was encrypted using a password and one or more certificates—and at least one of those certificates is already available on the computer—no decryption prompt occurs. The **Removable Storage Extractor** dialog appears (Figure 5.11) at once. The recipient can go to “Certificates Only” on page 59 and follow the instructions for extracting the archive.

**Password and Certificates: Certificates Not Available**

If the archive was encrypted using a password and one or more certificates—and none of the required certificates are available on the computer yet—the **Removable Storage Extractor** dialog appears with a choice of decryption methods: password or certificate(s).

![Removable Storage Extractor](image)

**Figure 5.12—Self-Extracting Archive, Decryption, Password/Certificate Prompt**

From the **Removable Storage Extractor** dialog, the recipient types the location where they want to save the decrypted file(s) in the **Extract to** field. Alternatively, they can browse to the location in the **Folders/Drives** pane.

To create a new folder or subfolder, the recipient selects an existing folder then clicks the **New Folder** button. At the **Create Folder** dialog, the recipient types the name for the new folder and click **OK**. The new folder is created in the specified location.
If the recipient has already decrypted the file in this location and wants to replace the previously decrypted file(s) with a more recent version, they select the **Overwrite existing files** check box. The files will be overwritten without warning. If the recipient does not select the **Overwrite existing files** check box and the files already exist in the specified location, the recipient will be warned that the files exist and given a chance to confirm or deny that they would like to continue with the action.

If the recipient selects the **Password** option, they enter the password under which this archive was encrypted, then clicks **Extract**.

If the recipient selects the **Have certificate on a smart card** option, the recipient then:

1. Inserts the smart card.
2. Clicks **Extract**. The token software prompts them for their PIN. Once the recipient authenticates, the certificates are read into the local certificate store, making them available for decryption.

Extraction begins. If an error occurs during extraction, a message appears for each file affected. If extraction is successful, the message, “The files/folders have been successfully extracted” appears. The recipient clicks **OK**; the message and the **Removable Storage Extractor** dialog exit.
6. Removable Storage Access Utility

Overview

Basics
The Removable Storage Access Utility allows you to encrypt and decrypt files on computers not protected by Removable Storage—except when launched from CD/DVD. Only decryption can be performed from CD/DVD media.

If your administrator has chosen to provide the Removable Storage Access Utility to you, it will be written automatically to removable media each time you connect your removable storage device to your Removable Storage–protected computer. The Removable Storage Access Utility will not be encrypted when it is written to removable media.

Two versions of the Removable Storage Access Utility exist: one for the Windows operating system and one for the Mac OS X operating system. Your administrator could have chosen to have Removable Storage copy both versions, only one version or the other, or neither version.

When a Removable Storage Access Utility is written to a device, a message is displayed, notifying you that this has occurred.

The Removable Storage Access Utility can only be used on computers not protected by Removable Storage. Only Windows, Mac OS X v10.5, and Mac OS X v10.6 operating systems are supported.

The Removable Storage Access Utility is designed to serve as your primary means of browsing and accessing the files on your removable storage device. Though the navigation tools provided by your operating system (Windows Explorer, Mac OS X Finder) allow you to browse the contents on your removable storage device, they won’t decrypt encrypted files or encrypt files for secure transport, as the two versions of the Removable Storage Access Utility do. They also will not remind you to encrypt unencrypted files before removing your device, as the Removable Storage Access Utility for Windows does.
Launching the Utility

Via AutoPlay

If the Windows AutoPlay feature is enabled, you will be prompted to launch the Removable Storage Access Utility each time you insert your removable device into a PC not protected by Removable Storage.

Click **Launch SEE-RS Access Utility** to open the Removable Storage Access Utility.

Other than the option to launch the Removable Storage Access Utility, the contents of the AutoPlay dialog will vary depending on your computer’s configuration.

Manual

To launch the Removable Storage Access Utility manually, browse to the device.

- From a PC, double-click or otherwise launch the Symantec Endpoint EncryptionRemovableStorageAccess.exe file.
- From a Mac, click or otherwise launch RSMacAccessUtility.dmg. Then double-click the RSMacAccessUtility.

Device Default Password

Basics

If you are using passwords to encrypt and want to use the same password to encrypt all of your files during this session, consider setting a Device Default Password. Setting a Device Default Password will eliminate the need for the Removable Storage Access Utility to prompt you for a password each time it attempts to encrypt a file.

Setting a Device Default Password can also reduce or eliminate decryption prompts, as the Removable Storage Access Utility will try to use the Device Default Password to decrypt before prompting you.

The Device Default Password will be used as long as the Removable Storage Access Utility remains open. It is cleared when the Removable Storage Access Utility is closed. To stop using the Device Default Password temporarily, you can suspend it.
The Device Default Password must adhere to any password requirements set by your administrator. These requirements will be displayed at the time that you set the password.

If you launch the Removable Storage Access Utility from CD/DVD, this feature will not be available.

**Set or Modify from File Menu**

To set or modify a Device Default Password for this Removable Storage Access Utility session, select **Set/Modify Device Default Password** from the **File** menu.

If your administrator has only enabled the use of certificates for encryption, the **Set/Modify Device Default Password** menu option is disabled. You may, however, set a Device Default Password any time you attempt to decrypt a file that was encrypted with a password. Skip to “Set or Modify from Password Decryption Prompt” on page 65.

The **Symantec Endpoint Encryption Access Utility Device Default Password Setup** dialog appears.

![Removable Storage Access Utility Device Default Password Setup](image)

Figure 6.3—Removable Storage Access Utility, Device Default Password Setup

In the **Password** field, type a password. In the **Confirm** field, type the password again. The password must conform to the password requirements listed on the screen, if any.

Click **OK**. If the password is invalid, you receive an error message that restates the requirements. Click **OK** to dismiss the message. Correct the password then click **OK** again.

If the password is valid, a success message displays.

To change the password, set it again.
Set or Modify from Password Decryption Prompt
You may set or modify a Device Default Password whenever you are prompted for a password to decrypt a file that was encrypted with a password.

From the Enter Password dialog, type the password into the Password field, select the check box for Make this password as device default password, then click OK. The Device Default Password is set.

Suspend
To suspend the Device Default Password, select Suspend Device Default Password from the File menu. A dialog confirms that the password is now suspended.

Reinstate
To reinstatement the current suspended Device Default Password, select Reinstall Device Default Password from the File menu.
Decryption

Basics
The Removable Storage Access Utility provides two methods of decrypting encrypted files. You can either work with the encrypted file from the device itself (“Open” on page 66), or you can decrypt the file to another location (“Decrypt to Location” on page 66).

Before an encrypted file can be decrypted, the credentials used to encrypt it will be necessary. These credentials may already be available, if one or more of the following is true:

- You set a Device Default Password that is the same as the password used to encrypt the file.
- You have already provided the password that was used to encrypt the file for a previous decryption.
- The certificate used to encrypt the file resides on a token which you have already inserted.
- The certificate used to encrypt the file exists in your local certificate store.

If none of the previous statements is true, you will be prompted to provide the credentials that were used to encrypt the file (“Decryption Prompts” on page 67).

Open
To work with the file from the device itself, either double-click or right-click and select Open. If you are prompted for credentials, refer to “Decryption Prompts” on page 67.

The file will be opened as a read-only file. After opening the file you may make modifications that you want to save. To accomplish this, select Save As. Using Save As, you can save your file back to the device or another location. If you save the file to another location, it won’t be encrypted. To achieve encryption of the file, you should save the file back to the device.

Decrypt to Location
To work with a file or folder from a location other than the removable device, right-click the file or folder, point to Decrypt To, and select Location.
The **Browse For Folder** dialog appears.

![Browse For Folder dialog](image)

**Figure 6.7—Removable Storage Access Utility, Browse for Folder**

Browse to the appropriate location. This must be a location other than the removable device. To create a new folder or subfolder select an existing folder then click **Make New Folder**. A folder named New Folder appears under the selected folder. Right-click the new folder to rename it.

Once you have selected the destination of the decrypted file or folder, click **OK**.

**Decryption Prompts**

**Basics**

If the Removable Storage Access Utility cannot locate the credentials needed to decrypt a file, a decryption prompt will be displayed.

The decryption prompt will vary according to the policy in place on the machine that copied the Removable Storage Access Utility automatically.

- If the encryption method is passwords, refer to “Password Decryption Prompt” on page 68.
- If the encryption method is certificates, refer to “Certificates Only” on page 68.
- If the encryption method is password and/or certificates, refer to “Password and Certificates” on page 69.
Password Decryption Prompt

If your encryption method is passwords only, and your Device Default Password (if any) does not match the password that the file was encrypted under, the password decryption prompt will be displayed.

![Password Decryption Prompt](image)

Figure 6.8—Removable Storage Access Utility, Decryption Password Prompt

Type the password that the file was encrypted under.

If you enter the wrong password more than the specified number of **password attempts remaining**, you will be forced to wait one minute before trying again.

Select the **Make this password as device default password** check box to set your Device Default Password to the password typed in the **Password** box. If you launched the Removable Storage Access Utility from CD/DVD, the **Make this password as device default password** check box will not be available.

Certificates Only

If your encryption method is certificates and the certificate(s) that the file was encrypted under cannot be found in the local certificate store, you will be prompted to provide at least one of the certificates.

![Certificate Decryption Prompt](image)

Figure 6.9—Removable Storage Access Utility, Certificate Decryption Prompt

If you have the token that contains the correct certificate, insert your token then click **OK**. Your token software will read the token, then prompt you for your PIN. Once you authenticate to the token, the certificate is read into your local certificate store and provides the credentials that the Removable Storage Access Utility requires.

If you do not have the token, click **OK** to dismiss the message. You will see a message that the operation failed.
Password and Certificates

If your encryption method is passwords and/or certificate(s) and the credentials that were used to encrypt the file cannot be found, you will be prompted to provide the password or one of the certificates.

![Password and Certificate Prompt](image)

To provide the password, select the **Password** option, then type the password. If you enter the wrong password more than the specified number of **password attempts remaining**, you will be forced to wait one minute before trying again. If you select **Make this password as device default password** your Device Default Password is set to the password that you enter. If you launched the Removable Storage Access Utility from CD/DVD, the **Make this password as device default password** check box will not be available.

To provide a certificate, select the **Have certificate on a smart card** option, insert the token that contains the correct certificate then click **OK**. Your token software will read it, then prompt you for your PIN. Once you authenticate to the token, the certificate is read into your local certificate store and provides the credentials that the Removable Storage Access Utility requires.

Encryption

Adding Files/Folders

To add new files and folders to your device, do any of the following:

- From a PC, drag the file(s) or folder(s) to the right pane of the Removable Storage Access Utility.
- From a PC, cut or copy the file to the Windows Clipboard, then select **Paste** from the **Edit** menu of the Removable Storage Access Utility.
- Open the **File** menu, point to **Add**, then right-click **Files** or **Folders**. An **Add Files** or **Browse For Folder** dialog box appears.
Before the files and/or folders are added to the Removable Storage Access Utility, a dialog appears prompting you to select an option: Encrypt or Don’t Encrypt.

To encrypt the file or folder, select Encrypt and click OK. You may be prompted to specify the credentials that you want to use to encrypt the file(s) (“PC Encryption Prompt” on page 72 or “Mac Encryption Prompt” on page 73, as appropriate to your operating system).

If you don’t want to encrypt the file or folder right away, select Don’t Encrypt and click OK.

If you launch the Removable Storage Access Utility from CD/DVD, this feature will not be available.

Manual Initiation
You can manually initiate the encryption at any time. To do so, first select the file(s) and/or folder(s). Then right-click and select Encrypt File/Folder.

Unless you are using passwords to encrypt and have set a Device Default Password, you will be prompted to specify the credentials that you want to encrypt the file(s) under (“PC Encryption Prompt” on page 72 or “Mac Encryption Prompt” on page 73, as appropriate to your operating system).
Encryption Reminder
Should you choose not to encrypt the files/folders at the time that you add them and neglect to manually initiate encryption during the session, you will be prompted when you select **Exit** from the **File** menu or when you click the close button.

![Encrypt On Close](image)

**Figure 6.12—Removable Storage Access Utility, Encrypt On Close**

Select the files that you would like to encrypt. If you want to encrypt them all, select the **Select All Files** check box. Click **Yes**. If you click **Yes** without selecting any files, you will receive this message: “You have not selected any file(s) to encrypt. Please select file(s) and try again.” Click **OK** to dismiss the message. Select one or more files, then click **Yes** again.

Unless you are using passwords to encrypt and have set a Device Default Password, you will be prompted to specify the credentials that you want to encrypt the file(s) under (“PC Encryption Prompt” on page 72 or “Mac Encryption Prompt” on page 73, as appropriate to your operating system).
PC Encryption Prompt

Basics

The Options dialog appears on a PC when you attempt to encrypt a file, but don’t have a Device Default Password set or are encrypting under certificates only.

![Options Dialog](image)

Figure 6.13—Removable Storage Access Utility, Encryption Prompt, PC

Its appearance will vary, depending on the policy in place on the machine that copied the Removable Storage Access Utility automatically. The policy in effect will be displayed at the top of the dialog.

### Table 6.1—Policy Statement and Effect on Options Dialog

<table>
<thead>
<tr>
<th>Policy Statement</th>
<th>Effect on Options Dialog</th>
</tr>
</thead>
<tbody>
<tr>
<td>You may encrypt your files using a password.</td>
<td><strong>Certificate</strong> area will be unavailable.</td>
</tr>
<tr>
<td>You may encrypt your files using a certificate only.</td>
<td><strong>Password</strong> area will not be displayed.</td>
</tr>
<tr>
<td>You may encrypt your files using a password, certificate, or both.</td>
<td>Both <strong>Password</strong> area and <strong>Certificate</strong> area will be displayed and available.</td>
</tr>
</tbody>
</table>

The name of the file that the Removable Storage Access Utility is attempting to encrypt will be displayed just below the policy statement.

**Selected File Area**

Select the check box in this area if you have selected multiple files for encryption and would like to use the same credentials to encrypt all of them.
Password Area
This area will only be available if the policy allows you to encrypt using passwords. Type and confirm a password in the Password and Confirm fields. Remember that if your administrator established password requirements for your Removable Storage account, those requirements apply to this encryption password as well.

If you additionally select the Make this password as device default password check box, then the password that you enter in the Password field will become your Device Default Password, as if you had selected Set/Modify Device Default Password from the File menu (“Set or Modify from File Menu” on page 64).

Certificate Area
This area will only be available if the policy allows you to encrypt using certificates. The Certificate area will display the certificates found in the local certificate store of your computer.

If no certificates exist in your local certificate store, you will need to insert your token and authenticate with your PIN. The token software reads the certificates into your local certificate store.

Click each check box under the Select column for the certificate or certificates that you would like to use. To see specifics about any certificate, click on the row, then click View Details. You can encrypt the file(s) under one or more (up to 10) certificates.

Conclusion
If you change your mind, you can cancel out of the process. If more than one file was selected in the Removable Storage Access Utility for encryption, and you have decided not to encrypt any of the files at this time, click Cancel All. If more than one file was selected for encryption and you have changed your mind about only the file displayed just above the Selected File area, click Cancel.

If you have not changed your mind, click OK. You receive a success message when encryption completes. If one file was encrypted, the file name appears in the message; if multiple files were encrypted, the number of files appears.

If you were encrypting files from the Encrypt On Close dialog, the application closes.

Mac Encryption Prompt
The password encryption prompt appears on a Mac when you attempt to encrypt a file, but don’t have a Device Default Password set.

Figure 6.14—Removable Storage Access Utility, Encryption Prompt, Mac
Type and confirm a password in the Password and Confirm Password fields. Remember that if your administrator established password requirements for your Removable Storage account, those requirements apply to this encryption password as well.

Select the Use the same password for all the files check box if you have selected multiple files for encryption and would like to use the same credentials to encrypt all of them.

Select the Make this password as device default password check box to caused the password that you enter in the Password field to become your Device Default Password, as if you had selected Set/Modify Device Default Password from the File menu (“Set or Modify from File Menu” on page 64).

**File or Folder Delete**

To remove a file or folder from the removable device, select the file or folder, right-click it and select Delete. You will be asked to confirm that you really want to delete the item.

![Figure 6.15—Removable Storage Access Utility, Confirm Delete](image)

Click Yes. The file is deleted.

If you launch the Removable Storage Access Utility from CD/DVD, this feature will not be available.

**Clean Up Temp Files Prompt**

When used on a PC, the Removable Storage Access Utility makes use of a temporary directory as it encrypts and decrypts files. Normally, the utility cleans up these temp files. However, if you select Exit from the File menu or click the close button while the utility is still working, you may see the following message:

![Figure 6.16—Removable Storage Access Utility, Delete Temp Files Request, PC](image)
To keep your data secure, make sure to go to the temp directory and remove all files.
7. CD-DVD Burner

Overview
The CD-DVD Burner application included with Removable Storage allows you to burn files to CD or DVD. If your workstation is protected by a policy of encrypting all files written to removable media or of encrypting new files written to CD/DVD media, the files that you burn will be encrypted.

Burning a Disc

Prerequisite
If you are using an external CD/DVD drive, make sure that the device is connected and has been recognized by Windows.

Navigation
To launch the CD-DVD Burner, click Start, point to All Programs, point to Symantec Endpoint Encryption Client, and select Removable Storage CD-DVD Burner. Alternatively, right-click the Symantec Endpoint Encryption icon in the Windows notification area and select Launch Removable Storage CD-DVD Burner.

![CD-DVD Burner Interface](image)

The Destination Drive drop-down list displays all of the available CD/DVD drives. Select the appropriate destination.
The **Policies** box indicates whether or not files burned to disc will be encrypted and if the Removable Storage Access Utility for Windows and/or the Removable Storage Access Utility for Mac OS X will be copied to the disc.

Locate the files and/or folders that you want to burn in Windows Explorer or on your desktop. Drag them to the **Files and/or folders to be burned** list. Once the mouse arrow changes to an add symbol, drop the files and/or folders.

Alternatively, click the **Add Files** or **Add Folder** button. Browse to the location of the files or folders that you want to burn in the dialog.

Double-click any folder to view its contents. The files appear in the **Files and/or folders to be burned** list.

To sort the **Files and/or folders to be burned** list by file/folder name or size in ascending or descending order, click on the **File/Folder** or **Size** column heading, as desired. An arrow appears in the column heading indicating the sort sequence.

To remove files or folders from the list, highlight them, and click the **Clear Data** button.

To name the CD or DVD, type a label in the **Disc Volume Label** field. A label is not required. If you do not label the disc, the default label with an encryption policy in place is `RS-Encrypted Disc yyyy-mm-dd`; without an encryption policy, the default label is `yyyy-mm-dd`.

To start the burn and/or encryption process, click the **Burn** button. The **Progress** and **Activity Details** indicate the status of the process. The **Burn** button changes to a **Stop Burn** button. To cancel the process, click the **Stop Burn** button.

If you have set Default Passwords, Default Certificate(s) or both, they will be used automatically to encrypt the file(s) on the CD or DVD. If you have not set any Default Passwords and/or Default Certificates, you will be prompted to specify a password and/or certificates. Each file in this session is encrypted with the password and/or certificate(s) you select. When all of the files you selected are encrypted and written to the disc, a success message displays and the disc is automatically ejected.

After a disc has been burned, you will be asked if you want to burn the same data again. If you insert a new disc and click **Yes**, the same data will be burned to the new disc.

The Symantec Endpoint Encryption CD-DVD Burner does not support multiple sessions on a single CD or DVD; however, the application does support writing to rewritable CDs and DVDs. If data exists, you will be asked whether you would like to erase the existing data before the burn process begins.

If you encounter errors or warnings, refer to Appendix C “CD-DVD Burner Application” on page 91.
Appendix A. Multimedia File Types Excluded

Overview

Your administrator may have excluded one or more multimedia groups from mandatory encryption. The Removable Storage panel of the User Client Console (Chapter 3 “Removable Storage Panel” on page 31) provides the name of the multimedia group(s) that are excluded. This Appendix details the file types that belong to each multimedia group:

- Audio (“Audio” on page 78),
- Video (“Video” on page 79), and
- Image (“Image” on page 81).

Audio

The following table identifies the file formats that belong to the audio group.

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC</td>
<td>Advanced Audio Coding</td>
<td>AAC Audio file (MPEG ADIF/ADTS AAC, iTunes AAC-LC)</td>
</tr>
<tr>
<td>AIF</td>
<td>Audio Interchange File (Apple)</td>
<td>AIFF audio &amp; AIFF-C compressed audio</td>
</tr>
<tr>
<td>AIFF</td>
<td>Audio Interchange File Format (Apple)</td>
<td>AIFF audio &amp; AIFF-C compressed audio</td>
</tr>
<tr>
<td>APE</td>
<td>Compressed using Monkey’s Audio lossless compression algorithm</td>
<td>Monkey’s Audio APE File</td>
</tr>
<tr>
<td>ASF</td>
<td>Advanced Systems Format (Microsoft)</td>
<td>Microsoft ASF, WMA, WMV</td>
</tr>
<tr>
<td>AU</td>
<td>Simple audio file format (Sun Microsystems)</td>
<td>Audio</td>
</tr>
<tr>
<td>FLAC</td>
<td>Free Lossless Audio Codec (open source)</td>
<td>FLAC Audio</td>
</tr>
<tr>
<td>M4A</td>
<td>Compressed with the Apple Lossless Encoder (ALE); uses the Apple Lossless Audio Codec (ALAC), saved in the MPEG-4 container format.</td>
<td>ISO Media MPEG v4 system, iTunes AAC-LC (M4V)</td>
</tr>
<tr>
<td>MID</td>
<td>Musical Instrument Digital Interface</td>
<td>Standard MIDI data, RIFF (little/big-endian) data MIDI</td>
</tr>
<tr>
<td>MIDI</td>
<td>Musical Instrument Digital Interface</td>
<td>Standard MIDI data, RIFF (little/big-endian) data MIDI</td>
</tr>
<tr>
<td>MP1</td>
<td>MPEG-1 Audio Layer I compression</td>
<td>MPEG ADTS, layer I, v2</td>
</tr>
<tr>
<td>MP2</td>
<td>MPEG-1 Audio Layer II (ISO/IEC 11172-3) compression</td>
<td>MPEG ADTS, layer II, v1 v2</td>
</tr>
<tr>
<td>MP3</td>
<td>MPEG-1 Audio Layer 3 compression</td>
<td>MP3 file(ID3 or MPEG ADTS, layer III, v1 v2 v2.5)</td>
</tr>
<tr>
<td>OGG</td>
<td>Uses Ogg Vorbis compression</td>
<td>OGG Audio</td>
</tr>
<tr>
<td>RA</td>
<td>Created with RealPlayer, uses the Real compression algorithm</td>
<td>RealAudio sound file</td>
</tr>
<tr>
<td>RAM</td>
<td>Created with RealPlayer, uses the Real compression algorithm</td>
<td>RealAudio sound file</td>
</tr>
<tr>
<td>RIFF</td>
<td>Resource Interchange File Format</td>
<td>RIFF (little/big-endian) data WAVE audio</td>
</tr>
<tr>
<td>File Extension</td>
<td>File Description</td>
<td>File Format</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>RIFF</td>
<td>Resource Interchange File Format</td>
<td>Standard MIDI data, RIFF (little/big-endian) data MIDI</td>
</tr>
<tr>
<td>RM</td>
<td>RealPlayer media</td>
<td>RealMedia file</td>
</tr>
<tr>
<td>SDS</td>
<td>MIDI Sample DUMP Standard File, contains standardized System Exclusive (SysEx) messages</td>
<td>SDS Audio</td>
</tr>
<tr>
<td>SPX</td>
<td>Ogg Vorbis Speex File</td>
<td>OGG Audio</td>
</tr>
<tr>
<td>TTA</td>
<td>True Audio, free, real-time, lossless codec</td>
<td>MP3 file(ID3 or MPEG ADTS, layer III, v1 v2 v2.5)</td>
</tr>
<tr>
<td>VOC</td>
<td>used by Creative Labs hardware (Soundblaster)</td>
<td>VOC Audio</td>
</tr>
<tr>
<td>VOX</td>
<td>MetaVoice encoded audio file that uses a mathematical algorithm to simulate human speech; based on Dialogic Adaptive Differential Pulse Code Modulation (ADPCM)</td>
<td>VOX Audio</td>
</tr>
<tr>
<td>WAV</td>
<td>Waveform audio format/Audio for Windows</td>
<td>RIFF (little/big-endian) data WAVE audio</td>
</tr>
<tr>
<td>WAVE</td>
<td>Waveform audio format/Audio for Windows</td>
<td>RIFF (little/big-endian) data WAVE audio</td>
</tr>
<tr>
<td>WMA</td>
<td>uses Windows Media compression (Microsoft)</td>
<td>Microsoft ASF,WMA,WMV</td>
</tr>
<tr>
<td>WMV</td>
<td>based on the Microsoft Advanced Systems Format (ASF) container format and compressed with Windows Media compression</td>
<td>Microsoft ASF,WMA,WMV</td>
</tr>
</tbody>
</table>

**Video**

The following table identifies the file formats that belong to the video group.

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Description</th>
<th>File Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASF</td>
<td>Advanced Systems Format (Microsoft) container format primarily for streaming media</td>
<td>Microsoft ASF,WMA,WMV</td>
</tr>
<tr>
<td>F4V</td>
<td>Adobe Flash container (ISO/IEC 14496-12)</td>
<td>Macromedia Flash Data/Video</td>
</tr>
<tr>
<td>FLIC</td>
<td>Animation file created by Autodesk</td>
<td>FLIC animation</td>
</tr>
</tbody>
</table>
### Multimedia File Types Excluded

#### Table A.2—Video File Types (Continued)

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLI</td>
<td>Animation file created by Autodesk</td>
<td>FLIC animation</td>
</tr>
<tr>
<td>FLV</td>
<td>Flash video container</td>
<td>Macromedia Flash Data/Video</td>
</tr>
<tr>
<td>M2V</td>
<td>Video data only, encoded using MPEG-2 compression</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>M4P</td>
<td>Apple-protected video</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>M4V</td>
<td>Apple video file based on MPEG-4</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>MOV</td>
<td>compressed with proprietary Apple algorithm</td>
<td>multimedia movie, 4X Movie file</td>
</tr>
<tr>
<td>MP2</td>
<td>MPEG-2 compression</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>MP4</td>
<td>MPEG-4 compression</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>MPEG</td>
<td>MPEG-1 or MPEG-2 compression</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>MPG</td>
<td>MPEG-1 or MPEG-2 compression</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>RIFF</td>
<td>Resource Interchange File Format</td>
<td>multimedia movie, 4X Movie file</td>
</tr>
<tr>
<td>RIFF</td>
<td>Resource Interchange File Format</td>
<td>RIFF (little/big-endian) data AVI</td>
</tr>
<tr>
<td>RIFF</td>
<td>Resource Interchange File Format</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>RM</td>
<td>RealPlayer media</td>
<td>RealMedia file</td>
</tr>
<tr>
<td>RMVB</td>
<td>RealMedia Variable Bitrate</td>
<td>RealMedia file</td>
</tr>
<tr>
<td>SWF</td>
<td>Small Web Format, Flash animation</td>
<td>Macromedia Flash Data/Video</td>
</tr>
<tr>
<td>VOB</td>
<td>Video Object, for video, audio, subtitles, and menus in DVD videos</td>
<td>RIFF (little/big-endian) data wrapped MPEG-1 (CDXA), ISO Media MPEG v4 system (part 12 revision, version 1 &amp; 2, v7 XML, v7 binary XML, 3GPP, 3GPP mobile, 3GPP JVT A VC, iTunes A VC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
</tbody>
</table>
### Multimedia File Types Excluded

#### Table A.2—Video File Types (Continued)

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMA</td>
<td>Windows Media compression</td>
<td>Microsoft ASF, WMA, WMV</td>
</tr>
<tr>
<td>WMV</td>
<td>Windows Media video compression</td>
<td>Microsoft ASF, WMA, WMV</td>
</tr>
</tbody>
</table>

#### Image

The following table identifies the file formats that belong to the image group.

#### Table A.3—Image File Types

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMP</td>
<td>uncompressed raster image made up of rectangular pixels</td>
<td>PC bitmap data</td>
</tr>
<tr>
<td>CUR</td>
<td>cursor image or animation, used for Windows mouse pointer</td>
<td>MS Windows Cursor</td>
</tr>
<tr>
<td>EMF</td>
<td>Enhanced metafile, 32-bits, vector graphic (Microsoft)</td>
<td>Windows Enhanced Metafile (EMF) image data</td>
</tr>
<tr>
<td>FH9</td>
<td>Macromedia FreeHand 9 vector image</td>
<td>Macromedia FreeHand 9 Document image</td>
</tr>
<tr>
<td>GIF</td>
<td>Graphics Interchange Format bitmap image, lossless compression, up to 256 colors</td>
<td>GIF image data</td>
</tr>
<tr>
<td>ICO</td>
<td>Microsoft Windows icon image, contains two bitmaps</td>
<td>MS Windows Icon file &amp; resource</td>
</tr>
<tr>
<td>JNG</td>
<td>JPEG Network Graphics, raster image, lossy compression</td>
<td>JNG (multiple-)image data Network Graphics</td>
</tr>
<tr>
<td>JPEG</td>
<td>Joint Photographic Experts Group (ISO 10918-1), lossy compression, up to 24-bit color</td>
<td>JPEG image (2000, standard, HSI proprietary)</td>
</tr>
<tr>
<td>JPG</td>
<td>Joint Photographic Experts Group (ISO 10918-1), lossy compression, up to 24-bit color</td>
<td>JPEG image (2000, standard, HSI proprietary)</td>
</tr>
<tr>
<td>MDI</td>
<td>Microsoft Document Imaging format, raster image</td>
<td>Office document imaging file</td>
</tr>
<tr>
<td>MNG</td>
<td>Multiple-image Network Graphics, raster image</td>
<td>JNG (multiple-)image data Network Graphics</td>
</tr>
<tr>
<td>PGM</td>
<td>Portable gray map, 8-bit raster image</td>
<td>Netpbm PGM/PPM text &amp; rawbits data image</td>
</tr>
<tr>
<td>PNG</td>
<td>Portable Network Graphics, raster image, indexed colors, lossless compression</td>
<td>PNG image data</td>
</tr>
<tr>
<td>PPM</td>
<td>Portable pixmap, 24-bit raster image, uncompressed</td>
<td>Netpbm PGM/PPM text &amp; rawbits data image</td>
</tr>
</tbody>
</table>
### Table A.3—Image File Types (Continued)

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PSD</td>
<td>raster image containing Photoshop-specific elements</td>
<td>Adobe photoshop images</td>
</tr>
<tr>
<td>SGI</td>
<td>image file native to Silicon Graphics workstation</td>
<td>SGI image data</td>
</tr>
<tr>
<td>SVG</td>
<td>Scalable Vector Graphics, two-dimensional vector graphic</td>
<td>Scalable Vector Graphics</td>
</tr>
<tr>
<td>TIF</td>
<td>Tagged Image File Format, raster image (Adobe)</td>
<td>TIFF image data, little/big-endian</td>
</tr>
<tr>
<td>TIFF</td>
<td>Tagged Image File Format, raster image (Adobe)</td>
<td>TIFF image data, little/big-endian</td>
</tr>
<tr>
<td>WMF</td>
<td>proprietary Microsoft Windows meta file</td>
<td>MS Windows metafont</td>
</tr>
</tbody>
</table>
Appendix B. Token Usage

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

Token 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.

Token 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 **Next** or **Log On**. Do not remove the token until token reading is complete.

If you encounter token or certificate errors, refer to the appropriate section in Appendix C “Error Messages & Prompts” for possible causes and resolution, as follows:

- During registration or re-registration, refer to “Token Registration” on page 84.
- During User Client Console logon, refer to “User Client Console” on page 98.
Appendix C. Error Messages & Prompts

Overview

This appendix provides detailed information about the error messages you may receive while performing the following operations:

- Registering with Symantec Endpoint Encryption using a token ("Token Registration" on page 84);
- Logging on to the User Client Console with a token ("User Client Console Token Logon" on page 85);
- Using removable storage devices ("Removable Storage Service" on page 86);
- Using the CD-DVD Burner application ("CD-DVD Burner" on page 76); and
- Using the User Client Console ("User Client Console" on page 98).

Token Registration

If you are using a token to register with Symantec Endpoint Encryption, you may encounter one or more of the following messages. This section will help you figure out what to do in the event of an error during token registration.

Table C.1—Registration Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect PIN.</td>
<td>You entered an incorrect PIN.</td>
<td>Carefully re-enter your PIN; if you enter an incorrect PIN too many times, your PIN could become blocked. Click Next.</td>
</tr>
<tr>
<td>The PIN is blocked for this token.</td>
<td>The number of remaining attempts on your token is zero.</td>
<td>Follow the instructions for getting assistance. Your PIN is blocked and the token needs to be replaced or modified.</td>
</tr>
<tr>
<td>The token has been removed. Please reinsert the token.</td>
<td>You removed the token before the registration process completed.</td>
<td>Reinsert the token and leave it inserted until you click Finish on the final registration panel.</td>
</tr>
<tr>
<td>A certificate validation error has occurred. The token needs to be replaced or modified by an administrator. Please call the help desk for assistance.</td>
<td>Your token does not contain any certificate, or your token contains an invalid certificate.</td>
<td>Follow the instructions for getting assistance. Your token does not contain a valid certificate.</td>
</tr>
</tbody>
</table>
Table C.2 lists the error messages that may occur when you are trying to log on to the User Client Console using a token.

### User Client Console Token Logon

Table C.2—User Client Console Logon Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incorrect PIN.</td>
<td>You entered an incorrect PIN.</td>
<td>Check your PIN, then type your PIN again and click Log On. Take care as you type your PIN, since resubmitting the wrong PIN a number of times could result in a blocked PIN. If you are not sure of your PIN, contact the administrator who manages your token.</td>
</tr>
<tr>
<td>The PIN is blocked for this token.</td>
<td>The number of remaining attempts on your token is zero.</td>
<td>Follow the instructions in the error message for getting assistance. Your PIN is blocked and your token needs to be replaced or modified.</td>
</tr>
<tr>
<td>The program could not log you on.</td>
<td>You removed the token immediately after clicking Log On.</td>
<td>Reinsert the token and leave it inserted until you are logged on to the User Client Console.</td>
</tr>
</tbody>
</table>
Removable Storage Service

The Removable Storage service may generate error messages or prompts from time to time. The following table will help you figure out what to do in the event of an error.

Table C.3—Removable Storage Service Messages

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Access denied. You clicked cancel on a password or certificate prompt and then attempted to open a file on a removable storage device. Without the correct password or certificate, the file cannot be decrypted and access is denied.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>🔄</td>
<td>Please enter a password. Removable Storage is attempting to encrypt or decrypt a file.</td>
<td>You can avoid this prompt by specifying a Default Password.</td>
<td></td>
</tr>
<tr>
<td>🔄</td>
<td>Please enter a password to encrypt the file file name. Removable Storage is attempting to encrypt a file.</td>
<td>You can avoid this prompt by specifying a Default Password.</td>
<td></td>
</tr>
<tr>
<td>Severity</td>
<td>Message</td>
<td>Meaning</td>
<td>Action</td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td>!</td>
<td>Please enter the decryption password for the file file name.</td>
<td>Removable Storage is attempting to decrypt a file.</td>
<td>Provide the password that was used to encrypt the file.</td>
</tr>
<tr>
<td>!</td>
<td>Please select a certificate.</td>
<td>Removable Storage is attempting to encrypt or decrypt a file.</td>
<td>You can avoid this prompt by specifying one or more Default Certificate(s).</td>
</tr>
<tr>
<td>!</td>
<td>Please enter a password or select a certificate, or both.</td>
<td>Removable Storage is attempting to encrypt or decrypt a file.</td>
<td>You can avoid this prompt by specifying a Default Password and/or Default Certificate(s).</td>
</tr>
<tr>
<td>!</td>
<td>Please select no more than 10 certificates.</td>
<td>You have tried to encrypt a file with more than ten certificates.</td>
<td>Ten certificates is the maximum number of certificates that can be used to encrypt a file. Revise your selections accordingly.</td>
</tr>
<tr>
<td>!</td>
<td>A certificate is needed to decrypt the file file name. If you have a certificate on a smart card, please insert the card and then click Retry.</td>
<td>Removable Storage is attempting to decrypt a file that was encrypted with a certificate. The certificates installed on your machine do not match the certificate(s) that was used to encrypt the file.</td>
<td>If the certificate that was used to encrypt the file resides on a token, insert the token so that Removable Storage can attempt to decrypt the file with the certificate(s) on your token.</td>
</tr>
<tr>
<td>!</td>
<td>Applications may respond ungracefully to the cancelled file creation. File replacement operations may result in the loss of the original file, if the application does not restore the original in the event of file creation failure. Do you still wish to cancel?</td>
<td>You clicked Cancel when prompted to enter a password to encrypt a file. You are being warned that your file may be deleted if you proceed with the cancellation.</td>
<td>Click Yes to continue with the cancellation. Click No to return to the password prompt.</td>
</tr>
<tr>
<td>!</td>
<td>You have exceeded the maximum number of attempts allowed.</td>
<td>Removable Storage is attempting to decrypt a file and you supplied the wrong password the maximum number of times allowed. You must wait one minute before submitting a password again.</td>
<td></td>
</tr>
</tbody>
</table>

Table C.3—Removable Storage Service Messages (Continued)
### Table C.3—Removable Storage Service Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Warning]</td>
<td>All of your default certs have expired, and will not be used for encryption. You will need to specify encryption options for each file until your default settings are updated using the client console.</td>
<td>Removable Storage is attempting to encrypt a file but all of the Default Certificates specified in the User Client Console are invalid or have expired.</td>
<td>You should update the Default Certificates listed in the User Client Console so that they are valid. If you can’t do that right now, specify a valid certificate manually. Alternatively, you may be given the option to enter a password.</td>
</tr>
<tr>
<td>![Warning]</td>
<td>Number of your default certs have expired, and will not be used for encryption. Your remaining default certs and/or password will be used for encryption. Please update your default settings using the client console.</td>
<td>Removable Storage is attempting to encrypt a file but some of the Default Certificates specified in the User Client Console are invalid or have expired. Removable Storage will encrypt the file using those Default Certificates that are still valid.</td>
<td>Locate the invalid Default Certificates in the User Client Console and update them.</td>
</tr>
<tr>
<td>![Warning]</td>
<td>The Removable Storage Service has been started manually. The service may not function properly in this state. Please log out and log back in to restore the service to normal operation.</td>
<td>The Removable Storage Service was started manually. You will be prevented from accessing your removable storage devices. This is true, regardless of the access policy enabled.</td>
<td>Log off of Windows and log back on to correct the problem.</td>
</tr>
<tr>
<td>![Warning]</td>
<td>The password does not meet the minimum requirements. It must contain the following: <code>local password requirements</code></td>
<td>Removable Storage is attempting to encrypt a file but the password you provided does not meet the minimum password requirements.</td>
<td>Enter a password that meets the specified requirements</td>
</tr>
<tr>
<td>![Warning]</td>
<td>Your default password will expire in $n$ day(s). You can change the Default Password by going to the Symantec Endpoint Encryption Client console and selecting the Removable Storage Default Password link.</td>
<td>Your Policy Administrator applied password aging requirements to your Default Password. Your password will expire in the number of days shown. If it expires, you will not be able to use it to encrypt or decrypt files.</td>
<td>Change your Default Password as soon as possible using the User Client Console.</td>
</tr>
</tbody>
</table>
Table C.3—Removable Storage Service Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>You are required to change your Removable Storage Default Password because it has reached the maximum age defined by your administrator. Please go to the Removable Storage Password link within the Symantec Endpoint Encryption Client console and change your Default Password by typing in a new password and selecting 'OK'. Your current Default Password will no longer be able to be used effective with your next Windows session. Please select QuickHelp if you have any questions about what this means.</td>
<td>Your Policy Administrator applied password aging requirements to your Default Password. Your password expired during your Windows session. You can continue to use the password to encrypt and decrypt files for now, but once you log off Windows, the next time you log on your Default Password will be expired.</td>
<td>Go to the User Client Console and change your Default Password now.</td>
</tr>
<tr>
<td>!</td>
<td>Your Removable Storage Encryption Default Password has expired. Please go to the Symantec Endpoint Encryption Client console, select Removable Storage -&gt; Default Password in the navigation pane, and change your Default Password.</td>
<td>Your Policy Administrator applied password aging requirements to your Default Password. Your password has reached the maximum allowed age. You must change the password or you cannot use it to encrypt or decrypt files. Until you change it, you will be required to enter passwords manually.</td>
<td>Go to the User Client Console and change your Default Password now.</td>
</tr>
<tr>
<td>!</td>
<td>Please enter a password. You clicked OK on the encryption password prompt, but did not enter and confirm a password.</td>
<td>You clicked OK on the encryption password prompt, but did not enter and confirm a password.</td>
<td>Enter and confirm a password. You can avoid this message by specifying a Default Password.</td>
</tr>
<tr>
<td>!</td>
<td>The passwords you entered do not match. Please re-enter the passwords.</td>
<td>The values you entered in the Enter Password and Confirm Password fields on the encryption password prompt do not agree.</td>
<td>Enter the same password in both fields. You can avoid this message by specifying a Default Password.</td>
</tr>
</tbody>
</table>
### Table C.3—Removable Storage Service Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚫</td>
<td>The password does not meet the minimum requirements. It must contain the following: <em>local password requirements</em> Please choose a different password.</td>
<td>The password you entered could not be saved because it does not meet the password requirements.</td>
<td>Choose a different password that meets the password requirements. You can avoid this message by specifying a Default Password.</td>
</tr>
<tr>
<td>🚫</td>
<td>The password entered is invalid.</td>
<td>Removable Storage is attempting to decrypt a file and you supplied the wrong password.</td>
<td></td>
</tr>
</tbody>
</table>
# CD-DVD Burner Application

The CD-DVD Burner application may generate error or success messages or prompts from time to time. The following table will help you figure out what to do in the event of an error.

## Table C.4—CD-DVD Burner Application Messages

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>You must register with Symantec Endpoint Encryption before you can use this application for burning data to disc.</td>
<td>You must register before you can use the CD-DVD Burner application to burn data to disc.</td>
<td>Register with Symantec Endpoint Encryption.</td>
</tr>
<tr>
<td></td>
<td>Your access policy does not allow write access to removable media, so you cannot use this application for burning data to disc.</td>
<td>Removable Storage is enforcing a read-only access policy.</td>
<td>If you disagree with the policy that is in place, contact your administrator.</td>
</tr>
<tr>
<td></td>
<td>Disc burning engine could not be initialized successfully.</td>
<td>The CD/DVD Burner application was unable to initialize the disc burning engine.</td>
<td>Reboot your computer and try again.</td>
</tr>
<tr>
<td></td>
<td>The disc drive could not be used to burn the disc.</td>
<td>An incompatibility exists between your disc recorder’s burning capability and the inserted media.</td>
<td>Insert the type of media that the selected disc drive can write to or select a disc drive capable of burning to the desired type of media.</td>
</tr>
<tr>
<td></td>
<td>The application is unable to locate the disc burning drive which was selected earlier.</td>
<td>The CD/DVD Burner application could not find the disc recorder.</td>
<td>Verify that your computer has or is connected to a CD/DVD drive that is capable of burning discs.</td>
</tr>
<tr>
<td></td>
<td>Disc recordable drive could not be locked.</td>
<td>Another application or process has prevented the CD/DVD Burner application from gaining exclusive access to the disc recorder.</td>
<td>Quit the other application or process and try the operation again.</td>
</tr>
<tr>
<td></td>
<td>A fixed hard disk drive is required for storage of temporary data. Application could not locate a fixed hard disk drive and therefore cannot continue.</td>
<td>Your temporary data location could not be found or does not reside on a fixed hard disk drive.</td>
<td>Check your drive connections and/or contact your administrator.</td>
</tr>
<tr>
<td></td>
<td>Application could not locate a fixed hard disk drive with enough free space for storage of temporary data, so application won’t burn the disc.</td>
<td>Your temporary data location does not have enough free space for storage of temporary data.</td>
<td>Free up some space and try the operation again.</td>
</tr>
</tbody>
</table>
### Table C.4—CD-DVD Burner Application Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Error Icon]</td>
<td>Application found a fixed hard disk drive with enough free space for storage of temporary data, but you do not have write access on <code>temporary folder path</code> to temporary folder, so application won’t burn the disc. Please get the write access on this folder and try again.</td>
<td>The CD/DVD Burner application has found that you do not have write privileges to your temporary data location. The burn process cannot be attempted.</td>
<td>Log in as a different user or contact your administrator to increase your privileges. Alternatively, your administrator may choose to change your temporary data directory.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>Temporary folder <code>temporary folder path</code> could not be created at your temporary data location. Please make sure that no file or folder is being used by any application in this temporary folder location and try again.</td>
<td>The CD/DVD Burner application was unable to complete the burning process because it was unable to write to your temporary data location. Either another application was accessing the location at the same time or you do not have privileges to write to this location.</td>
<td>Ensure that no other applications are accessing the temporary data directory. Also verify or change your permissions. Then try again.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>Disc could not be burned with selected data because your temporary data location is EFS enabled.</td>
<td>The CD/DVD Burner application cannot use an EFS-encrypted temporary data directory.</td>
<td>Either turn off EFS protection for the temporary data directory’s parent folder, or manually relocate the temporary data directory by editing the TMP or TEMP environment variables.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>File <code>[path/]name of file or folder</code> to be burned, could not be encrypted due to security reason.</td>
<td>The CD/DVD Burner application was unable to encrypt the file specified, due to a lack of permissions.</td>
<td>Verify that your account has sufficient access rights to perform this operation.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>Temporary file could not be deleted.</td>
<td>The CD/DVD Burner application was unable to delete a temporary file.</td>
<td>Manually delete the temporary file.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>The disc that you have inserted is not writable. Please insert a blank or rewritable disc of type CD-R, CD-RW, DVD-R, DVD-RW, DVD+R, or DVD+R DL into drive.</td>
<td>You attempted to burn data to a disc that is not writable.</td>
<td>Remove the disc from the drive and insert a disc that is writable.</td>
</tr>
</tbody>
</table>
The disc volume label can have only alphanumeric and underscore characters. The disc volume label’s length can not be more than 32 characters. Please type a valid disc volume label.

You have selected one or more files with very long file name. Application could not shorten file(s) name in temporary data location. If file encryption policy is set then file’s name length can exceed 102 characters, otherwise it can not exceed 106 characters. Please rename the file(s) with long name and try again.

Selected file or folder [path]name of file or folder could not be copied at your temporary data location because path length is exceeding the limit (259 characters) imposed by Windows system. Please shorten the name of selected file/ folder or sub folder(s) and try again.

File “SEERemovableStorage AccessUtility.exe” can not be selected to be burned on the root of the burnt disc. This file is SEE-RS Access Utility application, which will be burned automatically on the root of the burnt disc.

You have entered invalid characters or too many characters in the Disc Volume Label field.

The file name exceeds the maximum number of characters allowed. Files that will be encrypted have a shorter file name length requirement (102 characters) because the CD-DVD Burner application adds a four-character extension of .xml.

The folder, subfolder, and file names concatenated into a single path name together exceed the Windows path-length limit of 259 characters.

You have attempted to copy the Removable Storage Access Utility to the disc, but the CD-DVD Burner application will burn the file for you automatically.

Do not manually select the Removable Storage Access.exe file to be burned. If a policy is enabled to copy the Removable Storage Access Utility to all removable devices, then the CD-DVD Burner application will copy and burn the file on the disc for you.
### Table C.4—CD-DVD Burner Application Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Error Icon]</td>
<td>File “Autorun.inf” can not be selected to be burned on the root of the burnt disc. File “Autorun.inf” will be burned automatically on the root of the burnt disc to run SEE-RS Access Utility application.</td>
<td>You have attempted to copy Autorun.inf to the disc, but the CD-DVD Burner application will burn the file for you automatically.</td>
<td>Do not manually select the Autorun.inf file to be burned. If a policy is enabled to copy the Removable Storage Access Utility to all removable devices, then the CD-DVD Burner application will copy and burn the file on the disc for you.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>File “Platform.ico” can not be selected to be burned on the root of the burnt disc. File “Platform.ico” will be burned automatically on the root of the burnt disc to run SEE-RS Access Utility application.</td>
<td>You have attempted to copy Platform.ico to the disc, but the CD-DVD Burner application will burn the file for you automatically.</td>
<td>Do not manually select the Platform.ico file to be burned. If a policy is enabled to copy the Removable Storage Access Utility to all removable devices, then the CD-DVD Burner application will copy and burn the file on the disc for you.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>The Removable Storage Access Utility could not be copied to disc.</td>
<td>Your policy specifies that the Removable Storage Access Utility should be automatically copied to removable media. The CD/DVD Burner application was unable to do so.</td>
<td>Reboot your computer and try again. If the problem persists, contact your administrator.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>The estimated size of data which will be burned on disc exceeds disc capacity. The data will not be burned to disc. Please remove some data from the list.</td>
<td>You have added files and/or folders to the Files and/or folders to be burned list box in excess of the free space on the disc.</td>
<td>Reduce the number of files in the Files and/or folders to be burned list box.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>Name of file or folder could not be encrypted. Please free up some space on your temporary data drive and try again.</td>
<td>There is not enough free space on your temporary data drive for the file or folder that you want to burn to be encrypted prior to burning.</td>
<td>Free up some space on your temporary data drive.</td>
</tr>
<tr>
<td>![Error Icon]</td>
<td>Selected file or folder [path/]name of file or folder could not be copied at your temporary data location. Please check the file or folder and try again.</td>
<td>The burn operation failed because the CD-DVD Burner application could not copy the data you selected to be burned to a temporary location in order to encrypt the data.</td>
<td>Verify that you have sufficient free space on your hard disk. If the problem persists, contact the appropriate administrator.</td>
</tr>
</tbody>
</table>
### Table C.4—CD-DVD Burner Application Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="https://example.com/icon" alt="" /></td>
<td>Selected file or folder [path]/name of file or folder cannot be copied at your temporary data location. Please check the file or folder and try again.</td>
<td>The burn operation cannot proceed because the CD-DVD Burner application cannot copy the data you selected to be burned to a temporary location in order to encrypt the data.</td>
<td>Verify that you have sufficient free space on your hard disk. If the problem persists, contact the appropriate administrator.</td>
</tr>
<tr>
<td><img src="https://example.com/icon" alt="" /></td>
<td>Removable Storage does not have a password to encrypt this file. You must specify a password or a Default Password before the data can be encrypted and burned to disc.</td>
<td>You have not set a Default Password for removable storage encryption and decryption, you were prompted to provide a password after clicking the <strong>Burn</strong> button, and you clicked the <strong>Cancel</strong> button on the password prompt, so the data cannot be burned to disc.</td>
<td>Either specify the password when prompted, or set a Default Password using the User Client Console.</td>
</tr>
<tr>
<td><img src="https://example.com/icon" alt="" /></td>
<td>Removable Storage does not have a certificate to encrypt this file. You must specify a certificate or a Default certificate before the data can be encrypted and burned to disc.</td>
<td>You have not set a Default Certificate for removable storage encryption and decryption, you were prompted to provide a certificate after clicking the <strong>Burn</strong> button, and you clicked the <strong>Cancel</strong> button on the certificate prompt, so the data cannot be burned to disc.</td>
<td>Either specify the certificate when prompted, or set a Default Certificate using the User Client Console.</td>
</tr>
<tr>
<td><img src="https://example.com/icon" alt="" /></td>
<td>Removable Storage does not have a Password and/or certificate to encrypt this file. You must specify a Password and/or certificate or a Default password and/or certificate before the data can be encrypted and burned to disc.</td>
<td>You have not set either a Default Password or a Default Certificate for removable storage encryption and decryption. You were prompted to provide a password and/or certificate after clicking the <strong>Burn</strong> button, and you clicked the <strong>Cancel</strong> button. The data cannot be burned to disc.</td>
<td>Either specify a password or certificate when prompted, or set a Default Password or Default Certificate using the User Client Console.</td>
</tr>
<tr>
<td><img src="https://example.com/icon" alt="" /></td>
<td>An error occurred during the encryption of the data.</td>
<td>The data that you want to burn could not be encrypted.</td>
<td>Click <strong>OK</strong>, then click the <strong>Burn</strong> button again. If the problem persists, reboot your computer and try again.</td>
</tr>
<tr>
<td><img src="https://example.com/icon" alt="" /></td>
<td>Drive can not be added to be burnt on disc.</td>
<td>You attempted to burn an entire drive, e.g., C: or D:.</td>
<td>Modify your selection to the folder level.</td>
</tr>
<tr>
<td><img src="https://example.com/icon" alt="" /></td>
<td>Data could not be added in the list to be burned.</td>
<td>The file or folder that you attempted to add could not be added for an unknown reason.</td>
<td>Check your file or folder to see if there is a problem with the source data and/or try again.</td>
</tr>
</tbody>
</table>
### Table C.4—CD-DVD Burner Application Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Error]</td>
<td>Disc could not be erased.</td>
<td>An attempt to erase a rewritable disc was unsuccessful.</td>
<td>Insert a different rewritable or write-once disc and try the operation again.</td>
</tr>
<tr>
<td>![Error]</td>
<td>Disc could not be ejected successfully.</td>
<td>A physical problem with your disk drive may exist that is preventing the CD/DVD Burner Application from ejecting your disk.</td>
<td>Try pressing the button to eject the disk. Reboot your computer. If this fails, contact your administrator.</td>
</tr>
<tr>
<td>![Error]</td>
<td>Disc could not be burned due to an error.</td>
<td>There was an unknown error with the disc recorder.</td>
<td>Reboot your computer. If the problem persists, your disc recorder may be faulty.</td>
</tr>
<tr>
<td>![Info]</td>
<td>A file or folder with name [path/file or folder name] has already been selected to be burned to disk. Therefore, it was not added to the list.</td>
<td>You tried to add a file or folder to the <strong>Files and/or folders to be burned</strong> list box that was already there. So the file or folder was not added again.</td>
<td>You may want to rename the file or folder and try again.</td>
</tr>
<tr>
<td>![Info]</td>
<td>You need to stop the burning process before closing the application.</td>
<td>You tried to close the CD-DVD Burner application while a burn operation was in progress.</td>
<td>If you want to stop the burning process and close the application, click the <strong>Stop Burn</strong> button and then close the application.</td>
</tr>
<tr>
<td>![Info]</td>
<td>Please place the disc in the drive and try again.</td>
<td>You clicked the <strong>Burn</strong> button when there was no disc in the drive.</td>
<td>Place a disc in the drive and click the <strong>Burn</strong> button again.</td>
</tr>
<tr>
<td>![Info]</td>
<td>Disc could not be used for burning data. Please try again with another disc.</td>
<td>The disc that you inserted in the drive cannot be used for burning data for a reason that is not specified.</td>
<td>Remove the disc from the drive and insert another disc.</td>
</tr>
<tr>
<td>![Info]</td>
<td>Please wait until application stops the disc burning process.</td>
<td>You tried to close the application before the disc burning process had stopped.</td>
<td>Wait for the message, “The disc burning process has been halted.” Then close the application.</td>
</tr>
<tr>
<td>![Info]</td>
<td>The disc burning process has been halted.</td>
<td>You clicked the <strong>Stop Burn</strong> button after you started to burn data to a disc, and then you clicked <strong>Yes</strong> on the confirmation message. The application has now succeeded in stopping the disc burning process.</td>
<td></td>
</tr>
<tr>
<td>![Info]</td>
<td>The application is unable to locate a drive capable of writing data to disc.</td>
<td>The CD-DVD Burner application could not find a drive that can be used to burn your data.</td>
<td>The CD-DVD Burner application didn’t find any disc recorders present. You may not have the necessary hardware to perform this operation, or else your operating system may be unaware of your hardware.</td>
</tr>
</tbody>
</table>
Please reduce the number of files selected and try again.

The number of files that you tried to add exceeds the maximum buffer size. Remove some files from your queue.

The data has been burned to disc successfully. Do you want to burn another disc with the same data? If yes then remove the burned disc and insert a new disc and click Yes.

If you want to burn another disc with the same data, remove the burned disc, insert a new disc, and click Yes.

You have selected one or more files with names that exceed 102 characters or path length in temporary data location is exceeding the 259 character limit imposed by Windows system. The extra characters will be removed automatically before the files are burnt to disc. Do you choose to continue?

You have added some files to be burned that have file names of more than 102 characters. Alternatively, the path to your temporary data drive combined with the file names exceeds the 259 character limit imposed by the Windows operating system. Click Yes to allow the CD-DVD Burner application to shorten the names automatically so that they do not exceed the maximum. Click No to cancel the burning of these files. Shorten the long file name(s) yourself then try again.

You have selected one or more EFS-encrypted files to be burned. EFS-encrypted file(s) will be decrypted by EFS before being burned. If SEE-RS is set to encrypt all files, the files will be encrypted by SEE-RS before being burned to disc. Do you choose to continue?

You have selected some Encrypting File System (EFS)—encrypted files to be burned. These files will be decrypted by EFS before they are burned. The files will be encrypted again by Removable Storage before they are burned if an encrypt all or encrypt new policy is in effect. Click Yes to continue with the decryption of the EFS-encrypted files and the possible (depending on your encryption policy) re-encryption by Removable Storage. To keep the EFS-encrypted files encrypted by EFS, click No.

Do you really want to stop the disc burning process?

You clicked the Stop Burn button after you started to burn data to a disc. Click Yes to stop the disc burning process; click No to continue the disc burning process.

---

### Table C.4—CD-DVD Burner Application Messages (Continued)

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>📜</td>
<td>Please reduce the number of files selected and try again.</td>
<td>The number of files that you tried to add exceeds the maximum buffer size.</td>
<td>Remove some files from your queue.</td>
</tr>
<tr>
<td>🤔</td>
<td>The data has been burned to disc successfully. Do you want to burn another disc with the same data? If yes then remove the burned disc and insert a new disc and click Yes.</td>
<td>You have successfully burned one or more files and/or folders to disc.</td>
<td>If you want to burn another disc with the same data, remove the burned disc, insert a new disc, and click Yes.</td>
</tr>
<tr>
<td>🤔</td>
<td>Your disc contains data. This data needs to be overwritten to burn the disc. Would you like to erase disc data?</td>
<td>You tried to burn data to a disc that already contains data.</td>
<td>Click Yes if you have inserted a rewritable CD/DVD and would like to proceed to erase the existing data and burn the new data. If the CD/DVD is not rewritable or if you would like to preserve the existing data, click No.</td>
</tr>
<tr>
<td>🤔</td>
<td>You have selected one or more files with names that exceed 102 characters or path length in temporary data location is exceeding the 259 character limit imposed by Windows system. The extra characters will be removed automatically before the files are burnt to disc. Do you choose to continue?</td>
<td>You have added some files to be burned that have file names of more than 102 characters. Alternatively, the path to your temporary data drive combined with the file names exceeds the 259 character limit imposed by the Windows operating system.</td>
<td>Click Yes to allow the CD-DVD Burner application to shorten the names automatically so that they do not exceed the maximum. Click No to cancel the burning of these files. Shorten the long file name(s) yourself then try again.</td>
</tr>
<tr>
<td>🤔</td>
<td>You have selected one or more EFS-encrypted files to be burned. EFS-encrypted file(s) will be decrypted by EFS before being burned. If SEE-RS is set to encrypt all files, the files will be encrypted by SEE-RS before being burned to disc. Do you choose to continue?</td>
<td>You have selected some Encrypting File System (EFS)—encrypted files to be burned. These files will be decrypted by EFS before they are burned. The files will be encrypted again by Removable Storage before they are burned if an encrypt all or encrypt new policy is in effect.</td>
<td>Click Yes to continue with the decryption of the EFS-encrypted files and the possible (depending on your encryption policy) re-encryption by Removable Storage. To keep the EFS-encrypted files encrypted by EFS, click No.</td>
</tr>
<tr>
<td>🤔</td>
<td>Do you really want to stop the disc burning process?</td>
<td>You clicked the Stop Burn button after you started to burn data to a disc.</td>
<td>Click Yes to stop the disc burning process; click No to continue the disc burning process.</td>
</tr>
</tbody>
</table>
**User Client Console**

The User Client Console may generate error messages or prompts from time to time. The following table will help you figure out what to do in the event of an error.

### Table C.5—User Client Console Messages

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Please correct the items highlighted in red.</td>
<td>The password you entered in the Default Password panel could not be saved because the values you entered in the <strong>New password</strong> and <strong>Confirm new password</strong> fields do not agree or the value you entered in the <strong>New password</strong> field does not meet the password requirements. Alternatively, the Default Password you entered could not be saved because it does not meet the password requirements.</td>
<td>Look for items highlighted in red to see what requires correction.</td>
</tr>
<tr>
<td>!</td>
<td>Password and Confirm password do not match. Please enter values again.</td>
<td>The Default Password you entered could not be saved because the values you entered in the <strong>Password</strong> and <strong>Confirm password</strong> fields do not agree.</td>
<td>Look for items highlighted in red to see what requires correction.</td>
</tr>
<tr>
<td>🚫</td>
<td>Incorrect password. Please try again.</td>
<td>You supplied the wrong password when attempting to log on to the User Client Console.</td>
<td>Look for items highlighted in red to see what requires correction.</td>
</tr>
<tr>
<td></td>
<td>Please enter a password.</td>
<td>You clicked <strong>OK</strong> on the encryption password prompt, but did not enter and confirm a password.</td>
<td>Enter and confirm a password. You can avoid this message by specifying a Default Password.</td>
</tr>
<tr>
<td>🚫</td>
<td>The certificate issued by <strong>issuer</strong> with serial number <strong>serial number</strong> is no longer available on this computer. It has been removed from the default certificates list.</td>
<td>One or more of your Default Certificates are no longer stored on your machine.</td>
<td>You may want to make a note of the serial number of the certificate that was removed. Otherwise, no action is required. The defunct certificates have been removed automatically.</td>
</tr>
<tr>
<td>🚫</td>
<td>The certificate with serial number <strong>serial number</strong> is no longer available on this computer. It has been removed from the default certificates list.</td>
<td>One or more of your Default Certificates are no longer stored on your machine.</td>
<td>You may want to make a note of the serial number of the certificate that was removed. Otherwise, no action is required. The defunct certificates have been removed automatically.</td>
</tr>
</tbody>
</table>
Please close the Administrator Client before launching the User Client.

The maximum number of Symantec Endpoint Encryption user accounts has been reached on this computer. If you need an account, please contact your Symantec Endpoint Encryption client administrator.

The default password was saved successfully.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Message</th>
<th>Meaning</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Please close the Administrator Client before launching the User Client.</td>
<td>The Administrator Client Console and the User Client Console cannot both be open at the same time. The User Client Console cannot be opened because the Administrator Client Console is already open.</td>
<td>Close the Administrator Client Console and then open the User Client Console.</td>
</tr>
<tr>
<td>🔄</td>
<td>The maximum number of Symantec Endpoint Encryption user accounts has been reached on this computer. If you need an account, please contact your Symantec Endpoint Encryption client administrator.</td>
<td>You have attempted to register with Symantec Endpoint Encryption, but there are no available slots for new users.</td>
<td>Contact your Client Administrator.</td>
</tr>
<tr>
<td>🔄</td>
<td>The default password was saved successfully.</td>
<td>The Default Password you set was saved successfully.</td>
<td></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.

### Default Password/Certificate
Registered users and Client Administrators have the option of setting a Default Password and/or Default Certificate(s) in the User Client Console. Removable Storage will use Default Passwords and/or Default Certificates for encrypting files. In addition, if the Default Password and/or Default Certificate(s) set in the User Client Console match the password or certificate(s) that a file was encrypted under, Removable Storage will decrypt the file without a prompt.

### Device Default Password
A password that can be used to encrypt and decrypt files written to and extracted from a removable storage device when using the Removable Storage Access Utility. This password allows you to define a password once so that you do not have to enter a password for every file and folder encrypted and decrypted during the session. The password can be set, changed, suspended, and reinstated at any time during the application session.
**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.

**Grace Restarts**
A grace restart allows Windows to load without requiring the first user to register.

**Lockout**
A lockout occurs if a computer fails to check in with the Symantec Endpoint Encryption Management Server within the prescribed interval. Users cannot gain access to Windows. Only a Client Administrator can log on. A user may be able to regain access to the computer by using the One-Time Password (OTP) feature with help desk assistance.

**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.

**Policy Administrator**
Performs centralized administration of Symantec Endpoint Encryption. The Policy Administrator updates and sets client policies, and also runs reports.

**Pre-Windows Environment**
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.

**Registration**
The process wherein users set their credentials so that they can gain access to their removable storage devices and the User Client Console. 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.

**Re-Registration**
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.

**Self-Extracting Executables**
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.
Session Default Password

Registered users and Client Administrators may have the option of setting up to two Session Default Passwords in the User Client Console. Unlike a Default Password, Session Default Passwords can be configured by policy to be inactivated or deleted at the end of your Windows session. Removable Storage will use Session Default Passwords for encrypting files, in addition to or in place of the Default Password and Default Certificates. If the Session Default Password matches the password used to encrypt a file, Removable Storage will decrypt the file without a prompt.

Single Sign-On (SSO)

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.

Symantec Endpoint Encryption Framework

Provides Symantec Endpoint Encryption–wide features, such as authentication methods and settings, as well as registered user and Client Administrator accounts and information.

Symantec Endpoint Encryption Password

Used by Client Administrators or Users to authenticate to the Administrator Client Console or User Client Console.

Temporary Data Directory

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.

Unregistration

The removal of a Symantec Endpoint Encryption registered user account, either manually by a Client Administrator or automatically by policy.

User

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.
Index

A
access policy
no access 1, 31, 32
read and write 1, 31, 32
read only 1, 31, 32, 91
Authenti-Check 2, 17, 20, 21, 24, 30
guidelines 13, 30
automatic authentication 2, 17

C
CD/DVD Burner
burning 77
description 76
CD/DVD Burner application
temporary data directory 102
certificate
Default 1, 2, 17, 35, 36, 77
local store 44, 45
Client Administrator 2

D
decryption
prompt
certificate 44, 86
password 44, 86, 90
password/certificate 45, 86
Default Certificates 100
Default Password
setting 34
used for CD-DVD Burner 77
default passwords policy
allow device session default passwords 33
Device Default Password 63
about 63
reinstate 65
set from encryption Options 73, 74
set or modify from decryption prompt 65
set or modify from File menu 64
suspend 65

E
EFS 97
encryption
about 1
double 3
policy 39
prompt
certificate 42, 87, 88
password 40, 87, 88
password/certificate 43, 87
encryption policy
CD/DVD only 1, 31, 32, 76
do not encrypt 32
encrypt all 1, 31, 32, 39, 97
encrypt new 1, 31, 32, 97
per DLP for Endpoint 32
user choice 32, 37

F
files, renamed 47
focus 24

G
grace restarts 2, 5
grace restarts, definition 101

J
JAWS 1

L
lockout
Check-In panel settings 21, 50, 52

M
Mac OS X Finder 62

N
navigation
direct access keys 24
TAB key 24

P
password
Default 1, 2, 15, 17, 34, 86, 87, 95, 98, 99
Device Default 63, 64, 65, 68, 69, 73, 74
registration 7
Session Default 15, 34
Symantec Endpoint Encryption 2, 7, 10, 17, 18, 26
PIN, prompt 11, 45
Policy Administrator 2
Quick Help, use 24

R
registered user
viewing accounts 25
registration 2, 5, 6, 7, 91
Authenti-Check 13
mandate 5
notification, grace restarts available 5
password 7, 9
token 10
Removable Storage Access Utility
decryption 66
duplicate file names 47
encryption 69
file or folder delete 74
launch 63
not for Removable Storage computers 62
self-extracting files instead 49
re-registration 15