Contents

Preface ................................................................................................................. 11

Legal Notice ........................................................................................................ 11

Technical Support ................................................................................................ 12
  Contacting Technical Support ........................................................................... 12
  Licensing and registration .............................................................................. 13
  Customer service ........................................................................................... 13
  Support agreement resources ......................................................................... 14

Chapter 1  Introduction ................................................................................. 15

  About Symantec Endpoint Encryption .......................................................... 15
  About the Symantec Endpoint Encryption Policy Administrator Guide .......... 16
  Before you begin .......................................................................................... 16

Chapter 2  Essential administration tasks .................................................. 17

  The Management Password ......................................................................... 17
    About the Management Password .......................................................... 17
    Changing the Management Password ................................................. 18
  Preparing for and recovering from disaster .............................................. 19
    About disaster recovery ........................................................................ 19
    Backing up your database and important data ................................... 20
    Protecting data on a client computer .................................................. 21
    Creating a Windows PE (WinPE) recovery disc or drive for client data recovery ................................................................. 22
    Configuring the Symantec Endpoint Encryption recovery features ........ 22
    Recovering after an interruption: the recovery sequence ..................... 23
    Recovering after an interruption: regaining database access ................ 24
  About Symantec Endpoint Encryption logs ............................................... 25
  If you are using Microsoft Windows Server 2008 or Windows Server 2012 ................................................................. 27
  About Administrative Server Roles ........................................................... 27
  Configuring Server Roles .......................................................................... 31
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 3</td>
<td>Understanding the Symantec Endpoint Encryption administrative policies</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>About administrative policies</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>About types of administrative policies</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>About install-time policies</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>About Active Directory policies</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>About native policies</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Differences between Active Directory policies and native policies</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>About the Symantec Endpoint Encryption policy options</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>About the Symantec Endpoint Encryption policy options available as install-time policies and as Active Directory or native policies</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>About identifying the policy for a task</td>
<td>54</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Creating Symantec Endpoint Encryption client installers</td>
<td>69</td>
</tr>
<tr>
<td></td>
<td>About client installers</td>
<td>69</td>
</tr>
<tr>
<td></td>
<td>About the installation settings wizards</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>Creating a Symantec Endpoint Encryption Client installation package</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Configuring the Management Agent installation settings</td>
<td>73</td>
</tr>
<tr>
<td></td>
<td>Configuring the Drive Encryption installation settings</td>
<td>76</td>
</tr>
<tr>
<td></td>
<td>Configuring the Symantec Endpoint Encryption for BitLocker installation settings</td>
<td>84</td>
</tr>
<tr>
<td></td>
<td>Configuring the Removable Media Encryption installation settings</td>
<td>86</td>
</tr>
<tr>
<td></td>
<td>About enabling features in the Symantec Endpoint Encryption Client installation package</td>
<td>93</td>
</tr>
<tr>
<td></td>
<td>Creating a Symantec Endpoint Encryption for FileVault installation package</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>Creating a Windows Password Reset Utility installation package</td>
<td>99</td>
</tr>
</tbody>
</table>
Chapter 5  Deploying new Symantec Endpoint Encryption clients ................................................................. 101
Deploying client packages using a third-party tool ................................................................. 101
Deploying new clients using Group Policy Objects ............................................................. 102
Installing the client software manually .............................................................................. 104
Installing the Windows Password Reset Utility on a client computer ........................................ 105
Deploying client installers using the command line .............................................................. 106

Chapter 6  Configuring the Symantec Endpoint Encryption policy options ......................................................... 109
About configuring the Symantec Endpoint Encryption policy options ........................................ 109
Accessing the Symantec Endpoint Encryption policy options .................................................. 111
Configuring the Management Agent policy options - process overview ............................................. 112
Configuring the Management Agent - Password Authentication policy options ....................... 113
Configuring the Management Agent - Communication policy options ...................................... 115
Configuring the Drive Encryption policy options - process overview ........................................... 115
Configuring the Drive Encryption - Client Administrators policy options, for adding or editing ......................................................... 117
Configuring the Drive Encryption - Client Administrators policy options, for deleting ...................... 121
Configuring the Drive Encryption - Registered Users policy options ............................................ 122
Configuring the Drive Encryption - Single Sign-On policy options .............................................. 125
Configuring the Drive Encryption - Self-Recovery policy options .............................................. 125
Configuring the Drive Encryption - Startup policy options ....................................................... 126
Configuring the Drive Encryption - Logon History policy options ............................................. 130
Configuring the Drive Encryption - Encryption policy options .................................................. 130
Configuring the Drive Encryption - Client Monitor policy options .............................................. 131
Configuring the Drive Encryption - Help Desk Recovery policy options ..................................... 132
Contents

Configuring the Drive Encryption - Self-Encrypting Drives policy options ................................................................. 132
Configuring the Drive Encryption - Windows Password Reset policy option ............................................................. 133
Configuring the Drive Encryption - Remote Decryption policy option ........................................................................ 134
Configuring the Removable Media Encryption policy options - process overview .............................................................. 134
Configuring the Removable Media Encryption - Access and Encryption policy options .............................................. 135
Configuring the Removable Media Encryption - Device and File Type Exclusions policy options ................................. 139
Configuring the Removable Media Encryption - Encryption Method policy options .................................................... 140
Configuring the Removable Media Encryption - Default Passwords policy options ...................................................... 140
Configuring the Removable Media Encryption - Recovery Certificate policy options .................................................. 142
Configuring the Removable Media Encryption - Portability policy options ................................................................. 144
Configuring the Removable Media Encryption - Expired Certificates policy options .................................................. 145
Configuring the Removable Media Encryption - Workgroup Key policy options .......................................................... 145
Configuring the Mac FileVault Client policy options - process overview ......................................................................... 146
Configuring the Mac FileVault Client - Introduction policy options ............................................................................. 147
Configuring the Mac FileVault Client - Institutional Recovery Key policy options ...................................................... 148
Configuring the Mac FileVault Client - Communication policy options ........................................................................ 149
Configuring the BitLocker Client policy options - process overview .................................................................................. 150
Configuring the BitLocker Client - Encryption and Authentication policy options ....................................................... 150
Configuring the BitLocker Client - Client Monitor policy options .................................................................................. 151
Chapter 7  Creating and managing Symantec Endpoint Encryption GPO and native policies ........................................ 153
   About policy creation and management ........................................... 153
   Managing GPOs - process overview ................................................ 154
   Creating and editing GPOs or restoring installation settings ............... 154
   Managing native policies - process overview ................................... 158
   Creating and editing native policies ............................................... 158
   Managing Symantec Endpoint Encryption policies on virtual
desktops ..................................................................................... 161

Chapter 8  Deploying Symantec Endpoint Encryption GPO and native policies ............................................. 165
   Deploying GPOs - process overview ............................................... 166
   About Active Directory Computers ................................................ 166
   Deploying GPOs ........................................................................... 167
   Forcing GPO updates .................................................................... 167
   About GPO priority sequence ......................................................... 168
   About GPO assignment verification ................................................. 168
   Deploying native policies - process overview ................................... 168
   About Symantec Endpoint Encryption Managed Computers
groups ......................................................................................... 169
   Creating Symantec Endpoint Encryption Managed Computers
groups .......................................................................................... 170
   Moving computers from a Symantec Endpoint Encryption Managed
   Computers group to another group ................................................. 171
   Deleting a computer from a managed computer group ...................... 172
   Searching for specific computers ................................................... 172
   About wildcard search characters .................................................. 173
   About assigning native policies ..................................................... 175
   Assigning native policies ............................................................. 175
   Forcing native policy updates ......................................................... 176
   About conflicting Symantec Endpoint Encryption policies ................. 176

Chapter 9  Using Autologon to bypass preboot authentication ............................................................... 177
   About the Autologon Utility ............................................................ 177
   Creating Autologon MSI files .......................................................... 178
   Installing an Autologon MSI file on a client computer ....................... 179
   Configuring the Drive Encryption - Autologon policy options .......... 179
Chapter 10  Using server-based commands ............................................. 183
   About server-based commands ..................................................... 183
   Issuing server-based commands to encrypt or decrypt fixed disk
drives - process overview ............................................................. 185
   Issuing server-based commands to encrypt or decrypt fixed disk
drives ................................................................................. 186
   Forcing a server-based command to execute on the client
computers ........................................................................... 188
   Issuing server-based commands to cancel a pending command .... 188
   Issuing the Change Web Access server command on client
computers ........................................................................... 191

Chapter 11  Viewing Symantec Endpoint Encryption reports ......................... 195
   About reports in Symantec Endpoint Encryption ......................... 195
   Permissions required to access reports ....................................... 196
   Types of reports ................................................................... 196
   Additional features in reports ................................................. 197
   Customizing the appearance of reports ...................................... 197
   Changing the columns that are displayed in a report ................. 198
   About the extended columns in reports .................................... 199
   Viewing reports in the Management Console .............................. 206
   Viewing the synchronization status of forests in Active
   Directory ............................................................................. 207
   Viewing the history of actions performed in the Management
   Console ............................................................................... 207
   Viewing the history of logged events on client computers .......... 209
   Viewing information about specific computers in Active
   Directory ............................................................................. 210
   Viewing the encryption status of computers that have either
   Drive Encryption or Removable Media Encryption
   installed ............................................................................. 212
   Viewing a list of computers that currently do not encrypt files
   on removable media devices ............................................. 214
   Viewing a list of computers whose fixed drives are currently not
   encrypted ............................................................................. 215
   Viewing a list of computers whose certificates expire within a
   specified number of days ....................................................... 217
   Viewing a list of computers on which a specified user is
   registered ............................................................................. 219
   Viewing a list of computers that do not have Drive Encryption
   installed ............................................................................. 220
Chapter 12 Providing recovery support to your users ................................. 247

About Symantec Endpoint Encryption Help Desk Recovery program ......................................................... 247
Providing Help Desk Recovery user assistance for Symantec Endpoint Encryption clients ........................................... 250
Providing One-Time Password user assistance for legacy Symantec Endpoint Encryption clients ........................................... 252
Providing Whole Disk Recovery Token user assistance for client computers ................................................................. 254
## Contents

- Providing Help Desk Recovery assistance for the Symantec Endpoint Encryption for FileVault users ................................................ 256
- Providing Help Desk Recovery assistance for the Symantec Endpoint Encryption for BitLocker users ................................................ 257
- Best practices for recovering data .................................................. 258
- Recovering the Macintosh encrypted disk ....................................... 259

### Chapter 13

**Upgrading clients to Symantec Endpoint Encryption**

11.1.2 ............................................................................. 261

- About upgrading your Microsoft Windows clients .................... 261
- Before upgrading your Microsoft Windows clients .................... 264
- Upgrading your Microsoft Windows clients ............................ 268
- Using Group Policy Objects when upgrading Microsoft Windows clients .......................................................... 272
- Upgrading Symantec Endpoint Encryption for FileVault clients .... 275

### Chapter 14

**Uninstalling the Symantec Endpoint Encryption client software** .............................................................. 277

- About uninstalling the Symantec Endpoint Encryption client ........ 277
- Uninstalling the Symantec Endpoint Encryption client software using the Control Panel .......................................................... 279
- About uninstalling the Symantec Endpoint Encryption client with a third-party tool .......................................................... 280
- About uninstalling the Symantec Endpoint Encryption client software using Group Policy Objects .......................................................... 281
- Uninstalling the Symantec Endpoint Encryption Client installation package using Group Policy Objects .......................... 282
- Deploying uninstallation scripts using Group Policy Objects .......................................................... 283
- Uninstalling the Symantec Endpoint Encryption client software using the command line .......................................................... 284
- Uninstalling Symantec Endpoint Encryption for FileVault ............. 286

### Appendix A

**Multimedia file types excluded in Symantec Endpoint Encryption** ................................................... 289

- Audio file types excluded ............................................................. 289
- Video file types excluded ............................................................. 292
- Image file types excluded ............................................................. 296

### Index ................................................................................................................... 299
Preface

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo, PGP, and Pretty Good Privacy are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. For more information on the Third Party Programs, see the Third Party Notice document for this Symantec product that may be available at http://www.symantec.com/about/profile/policies/eulas/.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

■ A range of support options that give you the flexibility to select the right amount of service for any size organization
■ Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
■ Upgrade assurance that delivers software upgrades
■ Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
■ Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

support.symantec.com

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/
Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan  customercare_apac@symantec.com
Europe, Middle-East, and Africa  semea@symantec.com
North America and Latin America  supportsolutions@symantec.com
This chapter includes the following topics:

- About Symantec Endpoint Encryption
- About the Symantec Endpoint Encryption Policy Administrator Guide
- Before you begin

About Symantec Endpoint Encryption

Symantec™ Endpoint Encryption v11.1.2 provides full disk encryption, removable media protection, and centralized management. Powered by PGP technology, the drive encryption client renders data at rest inaccessible to unauthorized parties on laptops and desktops. Removable Media Encryption functionality lets end users to move sensitive data onto USBs, external hard drives, and memory cards while management includes compliance-based and customizable reporting to let administrators confirm that systems were protected if a loss or theft occurs.

Key Features:

- **Built PGP Strong** – High performing, strong encryption, built with PGP Hybrid Cryptographic Optimizer (HCO) technology that utilizes AES-NI hardware within existing operating systems for even faster speeds.

- **Robust Reporting** – Compliance-based reports, customizable reporting helps ease the burden of proof for administrators to auditors and key stakeholders.

- **Automation** – Individual and group policies and keys can be synched with Active Directory to help speed deployments and reduce the burden of administration.

- **DLP Integration** – Blend Symantec’s market-leading Data Loss Prevention software with removable media encryption for an even stronger, user-friendly endpoint security solution.
For more information, see http://www.symantec.com/data-loss-prevention

Key Benefits:

- **User-Friendly** – Initial encryption speed varies to allow users to continue working while encryption happens in the background and single-sign-on (SSO) means less passwords to remember
- **Flexibility** – Support for multi-user and non-Active Directory environments
- **Transparent** – Invisible installation for end-users, that includes automatic encryption

### About the Symantec Endpoint Encryption Policy Administrator Guide

The *Symantec Endpoint Encryption Policy Administrator Guide* is intended for administrators who configure and update various Symantec Endpoint Encryption 11.1.0 policies through the Management Console.

As an administrator, you can perform centralized administration of Symantec Endpoint Encryption 11.1.0. You can perform the following tasks:

- Configure and update the Symantec Endpoint Encryption policy options.
- Issue server-based commands to encrypt or decrypt drives on the fixed disks as well as the Microsoft eDrive support – Opal v2 compliant drives.
- Run reports.
- Change the management password.
- Run the Help Desk Recovery Program.

### Before you begin

Ensure that the following prerequisites are met before you configure policies on the Symantec Endpoint Encryption Management Server:

- Symantec Endpoint Encryption Management Server is installed and configured
- Management Console is installed and configured
Essential administration tasks

This chapter includes the following topics:

- The Management Password
- Preparing for and recovering from disaster
- About Symantec Endpoint Encryption logs
- If you are using Microsoft Windows Server 2008 or Windows Server 2012
- About Administrative Server Roles
- Working with the Symantec Endpoint Encryption Database Maintenance snap-in

The Management Password

This section contains the following topics:

- About the Management Password
- Changing the Management Password

About the Management Password

The Management Password is an important part of installing and upgrading Symantec Endpoint Encryption. If you do not already have a Management Password, you are prompted to create one when you install Symantec Endpoint Encryption Management Server 11.1.2 for the first time. When you set the Management Password, it is encrypted and stored in the Symantec Endpoint...
The Management Password

Encryption database. You can change the Management Password at any time after installation, in the Management Console.

You are required to enter the Management Password to:

■ Install and upgrade Symantec Endpoint Encryption Management Server
■ Install and upgrade the Management Console
■ Access the Help Desk Recovery snap-in in the Management Console
■ Create the Autologon Utility installation package
■ Create the Windows Password Reset Utility installation package

Do not lose your Management Password. Symantec cannot recover this password if it is lost. If you lose your Management Password you must reinstall the Management Server.

Symantec recommends that you protect and store your Management Password in a safe location. You should establish a protocol within your organization for all Management Password changes. Use this protocol to prevent situations where multiple administrators could inadvertently change the Management Password and prevent other administrators from accessing the functions that they require.

See “Changing the Management Password” on page 18.

Changing the Management Password

You might need to change the Management Password in accordance with your organization's IT security policy, or for any other reason. When you change the Management Password, you do not have to perform any other actions. Enter the new Management Password the next time you access the Help Desk Recovery snap-in in the Management Console, or perform any action that requires it.

See “About the Management Password” on page 17.

The following procedure provides instructions for changing the Management Password that you created when you installed the Symantec Endpoint Encryption Management Server.
**Warning:** Do not lose your Management Password. Symantec cannot recover this password if it is lost. If you lose your Management Password you must reinstall the Management Server and all your clients.

Symantec recommends that you protect and store your Management Password in a safe location.

You should establish a protocol within your organization for all Management Password changes. Use this protocol to prevent situations where multiple administrators could inadvertently change the Management Password and prevent other administrators from accessing functions that they require.

**To change the Management Password**

1. In the navigation pane of the Symantec Endpoint Encryption Management Server, click **Symantec Endpoint Encryption Management Password**.
2. In the **Current management password** field, type the management password that is currently in use.
3. In the **New management password** field and the **Confirm new password** field, type the password that you want to use from now on.
4. Click **OK** to save the new Management Password.

---

**Preparing for and recovering from disaster**

This section includes the following topics:

- About disaster recovery
- Backing up your database and important data
- Protecting data on a client computer
- Creating a Windows PE (WinPE) recovery disc or drive for client data recovery
- Configuring the Symantec Endpoint Encryption recovery features
- Recovering after an interruption: the recovery sequence
- Recovering after an interruption: regaining database access

**About disaster recovery**

Various interruptions can affect business continuity and result in the need for disaster recovery. Interruptions can include power outages, IT system crashes, and natural disasters. To manage such situations, you need to establish a defined process that keeps your company up and running.
The IT environment that you configure and the backup processes that you define play an important role in the extent of data recovery that is possible. For example, an IT environment that consists of a single primary server for your enterprise offers the least amount of data recovery.

As an administrator, carefully review your IT environment and your backup-and-recovery procedures. Also, ensure that you have all of the licensing and technical components that mirror exactly the present system configuration and administration.

The following sections describe recommended practices to help you prepare and manage disaster recovery in your enterprise. Although an administrator can perform the following recommendations, you can contact Symantec Technical Support for any assistance with the process.

See “About Symantec Endpoint Encryption Help Desk Recovery program” on page 247.

See “Providing Help Desk Recovery user assistance for Symantec Endpoint Encryption clients” on page 250.

See “Providing Whole Disk Recovery Token user assistance for client computers” on page 254.

See “Providing One-Time Password user assistance for legacy Symantec Endpoint Encryption clients” on page 252.

**Back up your database and important data**

**Goal:** To protect databases and data loss that can be caused by a variety of failures

**Recommended strategies:**

- Back up your database on a regular basis, preferably weekly.  
  Best practice: Back up your database immediately following the successful installation and configuration of the Symantec Endpoint Encryption Management Server.

- Back up critical data, including:
  - The Symantec Endpoint Encryption Management Password
  - Certificates, including the Removable Media Encryption Recovery Certificate
  - Configuration files
  - Registry files
  - License files
  - Log files
The IP address and host name of the Symantec Endpoint Encryption Management Server

Store the backed-up files off-site at a secure location.

**Caution:** When you back up database files to a secure location, ensure that the files are copied properly. If the copied files are corrupt, you cannot restore your database.

- Test your backup strategy: restore a set of backups and then recover your database
  - Testing helps to ensure that you have the required backups to recover from various failures. Testing also ensures that your procedures can be executed effectively when a real failure occurs.

See “About the Management Password” on page 17.


See the *Symantec Endpoint Encryption Installation Guide*.

## Protecting data on a client computer

**Goal:** To prevent data loss if a computer is lost or stolen, or if you cannot decrypt the disk

**Recommended strategies:**

- Implement a strategy such that your users back up all data on their disk, before installing Symantec Endpoint Encryption Drive Encryption.

- Institute a procedure so that users regularly back up their disks.

- For users of previous versions of Symantec Endpoint Encryption on unmanaged client computers, recommend that they save the Whole Disk Recovery Token (WDRT) token. They should save the file to a secure off-site location. The WDRT allows data to be accessed on unmanaged computers if a user forgets their Windows password and cannot authenticate to the preboot login screen. The WDRT also protects users who have the Drive Encryption Self-Recovery feature available, but who have forgotten the answers to the defined questions. Without the WDRT, data can be lost.

- When you restore client data, make sure that you do not mix different scenarios that you may have used for backing up data and restoring data. For example, if you used an unmanaged client to back up the files, use an unmanaged client to restore the files.
Creating a Windows PE (WinPE) recovery disc or drive for client data recovery

Goal: To protect and make accessible the data on encrypted client computers that cannot boot

Recommended strategies:

■ Create a Windows Preinstallation Environment (Windows PE or WinPE) CD or UFD (USB flash drive).
  ■ A customized WinPE CD or UFD is the only way to recover your data from a computer that cannot load a Microsoft Windows operating system.
  ■ As a best practice, create the customized WinPE CD or UFD immediately after installing the client software.

■ Use a WinPE CD or UFD:
  ■ As a startup recovery tool. Use the created WinPE CD or UFD to gain access to data on the computers that cannot load the Windows operating system and start properly.
  ■ To restore the previous master boot record (MBR) of a client computer, after you restore the computer from a volume backup.
  ■ To decrypt an encrypted disk using the administrator access credentials and recover data from a locked client computer.


Configuring the Symantec Endpoint Encryption recovery features

Goal: To understand the built-in recovery features and to create an efficient data loss prevention plan

Proposed strategies:

■ Become knowledgeable about the Symantec Endpoint Encryption built-in recovery features. They include:
  ■ Drive Encryption Self-Recovery
  ■ Help Desk Recovery
  ■ Recovery certificates
Drive Encryption Self-Recovery (administrator task): enable and configure this feature.
Ensure that the Drive Encryption Self-Recovery feature is enabled on all the client computers, by selecting this policy option. A user can answer the Drive Encryption Self-Recovery questions to gain access to their system, if they forget their authentication password.

Drive Encryption Self-Recovery (user task): Recommend that all new users know what the supported languages and characters are in their preboot environment. Have them create self-recovery answers immediately when prompted after the installation of Drive Encryption. Depending on how their policy is set, they may first need to define the questions as well.

Help Desk Recovery: enable and configure this feature.
With Help Desk Recovery enabled on a client computer, the user can access their encrypted computer under two conditions. One condition is that the user forgot their password. The other condition is that the computer is in a lockout state at preboot. This access is done with help desk assistance.

Recovery certificate: enable this encryption policy option for Removable Media Encryption.
Removable Media Encryption encrypts a file with a recovery certificate, in addition to the password or certificate that is set on a computer. The recovery certificate provides an option to recover an encrypted file in case the password or the certificate that was used for encryption is lost.
Removable Media Encryption encrypts a file with the public key of the recovery certificate. You or a client administrator can then use the copy of the recovery certificate that includes the private key to recover an encrypted file.

See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.
See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 132.
See “Best practices for using a recovery certificate” on page 143.

Recovering after an interruption: the recovery sequence
Symantec recommends that you adhere to the recommended disaster recovery preparation and strategies. If you do encounter an interruption and need to recover, follow this recovery sequence:

1. Restore the Symantec Endpoint Encryption Management Server.
2. Restore the database and all the files and certificates.
3. Restore client communications.
   See “Recovering after an interruption: regaining database access” on page 24.

Recovering after an interruption: regaining database access

If you have lost access to your primary Symantec Endpoint Encryption database, you can access your backup database located at your disaster recovery site. From the Manager Computer, modify the fields when prompted to authenticate to the SQL server.

To regain database access:

1. Make sure your Windows account is not provisioned with rights to access the Symantec Endpoint Encryption database.
2. On the Manager Computer, attempt to launch the Management Console.
3. In the SQL Server Logon Information window, edit the **Server name** and **Initial catalog** fields to connect to your disaster recovery site.
   - For the **Server name**, the syntax is: `computer name, port number\instance name`
   - **Note:** The NetBIOS name of the server hosting the Symantec Endpoint Encryption database is always required. The TCP port number is only necessary if you are using a custom port. The instance name is only needed if you are using a named instance.

   - For the **Initial catalog**, enter the database name that you entered during Symantec Endpoint Encryption Management Server installation.
   - **Note:** The default name is `SEEMSDb`, but you may have changed the name.

4. For **Authentication Mode** select **Windows Authentication** or **SQL Authentication**.
5. In the **User name** field:
   - For Windows authentication, type the Windows account name in NetBIOS format.
   - For SQL authentication, type the SQL user name.
6. In the **Password** field, type the account password.
7. Click **Connect** to authenticate.
About Symantec Endpoint Encryption logs

The Symantec Endpoint Encryption logs record information about the various activities that are performed on Symantec Endpoint Encryption Management Server as well as activities that are performed using Drive Encryption, Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption on client computers. You can use these logs to understand and troubleshoot any issues. Symantec Endpoint Encryption provides the following logs:

- Symantec Endpoint Encryption Management Server logs
- Drive Encryption logs
- Symantec Endpoint Encryption for BitLocker logs
- Removable Media Encryption logs

The Drive Encryption, Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption logs are created on their respective client computers. As an administrator, you can view these logs for administrative or audit purposes.

Windows Event Logs for Drive Encryption, Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption are enabled by default. You do not need to create a registry key to enable event logs. Event logs are always logged with an appropriate severity. Event logs reside on the local client computer. You can view these event logs through the Windows Event Viewer. For example, you can view the Removable Media Encryption event logs to determine whether a file was encrypted so that the user’s data was not disclosed.

Debug logs are useful for troubleshooting the Symantec Endpoint Encryption application failures as it gives detailed logs of the activities. To make use of debug logs, you need to enable the debug logs on your Drive Encryption, Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption client computers. Download the Microsoft DebugView utility from the Microsoft TechNet website to view the Removable Media Encryption debug logs.

About the Symantec Endpoint Encryption Management Server logs

Symantec Endpoint Encryption Management Server logs are useful for troubleshooting any issues that are related to the web service. The 'Symantec.Endpoint.Encryption.GECommunicationWS' registry key controls the server logs. The Symantec Endpoint Encryption Management Server installer does not create this registry key. You need to manually create this registry key at the following location in the registry hive:
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Endpoint Encryption\Trace\TraceSinks\FileSink

The log file is located at the following path on the system where Symantec Endpoint Encryption Management Server is installed:

<ProductInstallDirectory>/Services/Logs

The default name of the log file is in the following format:

gecws_mm_dd_yyyy.txt.

**About the Drive Encryption logs**

The Symantec Endpoint Encryption Client installer creates a registry key for managing the Drive Encryption logs by default. These Drive Encryption logs are created at the following location:

Program Files\Symantec\Endpoint Encryption Clients\Management Agent\TechLogs

By default, the Drive Encryption log’s value is set to Warning. The Drive Encryption logs are named in the following format:

eedXXXYY.log,

where:

- XXX can be Service, AdminCLI, user, and so on
- YY is an integer value

**About the Symantec Endpoint Encryption for BitLocker logs**

The Symantec Endpoint Encryption for Windows installer creates a registry key for managing the Symantec Endpoint Encryption for BitLocker logs by default. The Symantec Endpoint Encryption for BitLocker logs are created at the following location:

Program Files\Symantec\Endpoint Encryption Clients\Management Agent\TechLogs

By default, the Symantec Endpoint Encryption for BitLocker log’s value is set to Warning. The Symantec Endpoint Encryption for BitLocker logs are named in the following format:

SymBitLockerServiceXX.log

BitLockerClientUIXX.log

where:
XX is an integer value

**About the Removable Media Encryption logs**

The Symantec Endpoint Encryption Client installer does not create the registry key for managing the Removable Media Encryption logs by default. You need to enable the debug logging for Removable Media Encryption.

For more information on enabling the Symantec Endpoint Encryption Management Server, Drive Encryption, and Removable Media Encryption logs, including information on the registry keys and logging levels, see the knowledge base article: Enabling Logging and Debug Logging in Symantec Endpoint Encryption v11.

---

**If you are using Microsoft Windows Server 2008 or Windows Server 2012**

*Note:* Starting with Symantec Endpoint Encryption 11.0.1, users are not required to install the Aero Desktop theme on Microsoft Windows Server 2008 R2 or Windows Server 2012 R2.

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

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

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

---

**About Administrative Server Roles**

The Symantec Endpoint Encryption Configuration Manager lets you assign Symantec Endpoint Encryption Management Server roles to an individual or a group of administrative users. You can assign these roles to an administrative user or a group of administrative users and provide application-level access and allow administrative users to access only certain server snap-ins, such as Help Desk.

The server roles are as follows:

- Server administrator
- Setup administrator
- Policy administrator
■ Report administrator
■ Help Desk administrator

**Server Role functions**

The following table lists the server roles and the Management Console snap-ins to which each server role allows access. The table also lists a summary of the functions that an administrator can perform with each snap-in.

**Table 2-1** Server Role functions

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Snap-in Access</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Symantec Endpoint Encryption Management Password</td>
<td>Set up and change the Management Password. The Management Password is required to:</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Encryption Management Server</td>
<td>■ Install and upgrade Symantec Endpoint Encryption Management Server</td>
</tr>
<tr>
<td></td>
<td>All other snap-ins as listed below</td>
<td>■ Install and upgrade the Management Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Access the Help Desk Recovery snap-in in the Management Console</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Create the Autologon utility installation package</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Create the Windows Password Reset Utility installation package</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the Management Password is lost, the Management Server must be reinstalled.</td>
</tr>
<tr>
<td>Symantec Endpoint Encryption Database Maintenance</td>
<td>View and remove old tracked endpoints and recorded client events from the database.</td>
<td></td>
</tr>
<tr>
<td>Server Role</td>
<td>Snap-in Access</td>
<td>Function</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Setup</td>
<td>Symantec Endpoint Encryption Software Setup</td>
<td>Create installation policies for the Management Agent, Drive Encryption, and Removable Media Encryption and generate client MSIs.</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Encryption Autologon Utility</td>
<td>Generate MSIs that enable or disable the autologon function on client computers. If autologon is enabled, users bypass preboot authentication.</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Encryption Windows Password Reset</td>
<td>Generate the Windows Password Reset Utility MSI that installs the Windows Password Reset feature on Drive Encryption client computers.</td>
</tr>
<tr>
<td>Server Role</td>
<td>Snap-in Access</td>
<td>Function</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy</td>
<td>Symantec Endpoint Encryption Native Policy Manager</td>
<td>Create and deploy native policies to client computers.</td>
</tr>
<tr>
<td></td>
<td>Active Directory Users and Computers</td>
<td>Manage users and computers in the AD hierarchy.</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Encryption Users and Computers</td>
<td>Manage users and computers in the SEE hierarchy.</td>
</tr>
<tr>
<td></td>
<td>Group Policy Management</td>
<td>Create and deploy GPOs to client computers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To access group policy management snap-ins without any issue user should be member of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>following four security groups:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 Domain Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Domain Users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 Enterprise Administrators</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 Group Policy Creator owners</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Encryption Server Commands</td>
<td>Issue server-based commands from the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The commands are to encrypt or decrypt fixed disk drives on specified client computers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The Symantec Endpoint Encryption Server Commands snap-in provides reports on issued commands.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>It also provides an interface for canceling pending commands.</td>
</tr>
</tbody>
</table>
Table 2-1  Server Role functions (continued)

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Snap-in Access</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report</td>
<td>Symantec Endpoint Encryption Reports</td>
<td>Run and customize predefined reports. View information about client computers, Active Directory and native policy settings, and Active Directory service synchronization. To access custom reports, the user must have administrative rights. Local users cannot access custom reports.</td>
</tr>
<tr>
<td>Helpdesk</td>
<td>Symantec Endpoint Encryption Help Desk</td>
<td>Use online or offline Help Desk recovery options to assist users to regain access to their computers from preboot, either because of a forgotten password or a computer lockout.</td>
</tr>
</tbody>
</table>

Configuring Server Roles

You can define server roles for individual Active Directory users, server administrator users, and assign roles to Active Directory groups. You can define the database access to users and groups and you can limit administrative access in the Management Console. This feature can be enabled or disabled by the server administrator. When you enable this feature, the logged in user is added as the Server Administrator role and has access to all snap-ins.

**To configure server roles for Active Directory users:**

1. On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.
2. Select **Server Roles** from the list on the left of the screen.
3. Switch the **Manage Server Roles** toggle to **On**.
4. Do one of the following:
   - Click **Add User** to add and configure a role to an Active Directory user.
   - Click **Add Group** to add and configure one or more server roles to a group.
5 Under **Select location**, browse to the Active Directory users.

6 Enter at least the first few letters of a user name or group name.

7 Click **Check name**.

8 Select one or more users or groups from the list.

9 To assign one or more roles to one or more selected users or group, under **Assign Role**, click one or more check boxes next to the roles.

10 Click **Add**.

11 Click **Allow Symantec Endpoint Encryption to manage database access permissions for AD users** to enable Symantec Endpoint Encryption to configure and manage SQL server logins and database access permissions for Active Directory users.

   **Note:** Make sure that the user who authenticated to the database has the appropriate roles and permissions to manage SQL Server database users.

12 Click **Save**.

**To configure server roles for Local Users:**

1 On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.

2 Select **Server Roles** from the list on the left of the screen.

3 Switch the **Manage Server Roles** toggle to **On**.

4 Do one of the following:
   - Click **Add User** to add and configure a role to a local user.
   - Click **Add Group** to add and configure one or more server roles to a group.

5 Under **Select location**, browse to the local users directory.

6 Enter at least the first few letters of a user name or group name.

7 Select one or more users or groups from the list.

8 To assign one or more roles to one or more selected users or group, under **Assign Role**, click one or more check boxes next to the roles.

9 Click **Add**.

10 Click **Save**.
Editing Server Roles

The server administrator can edit previously configured server roles for individual users or groups to change administrative access within the Symantec Endpoint Encryption Manager. The administrator can also configure and edit server roles for multiple users or groups.

To edit Server Roles:

1. On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.
2. Select Server Roles from the list on the left of the screen.
3. Select a user or a group from the list.
4. Click Edit.
5. Select the desired roles for this user or group from the Edit Role dialog box. The user’s current roles are preselected and can be deselected.
6. Click OK, and then click Save.

Note: It is possible to select multiple users to edit simultaneously. If you do, the dialog box is not populated with a user’s current server roles so your selection changes all of the users to have the same roles.

Removing User Accounts

The server administrator can remove previously configured server roles for individual users to eliminate specific administrative access within the Symantec Endpoint Encryption Manager.

To remove Server Roles:

1. On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.
2. Select Server Roles from the list on the left of the screen.
3. Select the user(s) from the list.
4. Click Remove.
5. Click Save.

Disabling Server Roles

The server administrator can disable the Server Roles feature at any time so that all users running the Configuration Manager have access to all snap-ins. Once
this feature is disabled, the user accounts are removed from the user interface but are not deleted from the database. If you re-enable the Server Roles feature, the previously assigned users are available.

To disable the Server Roles feature:

1. On the Symantec Endpoint Encryption Management Server, launch the Configuration Manager.
2. Select **Server Roles** from the list on the left of the screen.
3. Switch the **Manage Server Roles** toggle to **Off**.
4. Click **Save**.

**Note:** When the Configuration Manager is launched and server roles are enabled, the current user is automatically assigned to the server administrator role. This user can modify all other users but cannot change their own role.

---

**Working with the Symantec Endpoint Encryption Database Maintenance snap-in**

You can use the Symantec Endpoint Encryption Database Maintenance snap-in to view and remove old client check-in data and recorded client event data from the Symantec Endpoint Encryption Management Server database. This feature allows you to view and remove data that is older than one, two or three years.

To add the Database Maintenance snap-in:

1. In the Management Console, click **File > Add/Remove Snap-ins**.
2. In the **Add or Remove Snap-ins** dialog box, select the **SEE Database Maintenance** snap-in.
3. Click **Add**.
4. Click **OK**.

To view the number of client computer check-ins:

1. In the Management Console, select the Symantec Endpoint Encryption **SEE Database Maintenance** snap-in.
2. On the **Database Maintenance** page, click the arrow next to **Number of clients that have not checked in since**, select the number of years of data you want to view.
To delete client computer check-ins:
1. In the Management Console, select the Symantec Endpoint Encryption Database Maintenance snap-in.
2. On the **Database Maintenance** page, click the arrow next to **Number of clients that have not checked in since** and select the number of years of data you want to remove.
3. Click **Purge Clients older than <specified> Year**.
4. Click OK.

To view the number of recorded client events:
1. In the Management Console, select the Symantec Endpoint Encryption Database Maintenance snap-in.
2. On the **Database Maintenance** page, click the arrow next to **Number of client events older than** and select the number of years of data you want to view.

To delete recorded client events:
1. In the Management Console, select the Symantec Endpoint Encryption Database Maintenance snap-in.
2. On the **Database Maintenance** page, click the arrow next to **Number of client events older than** and select the number of years of data you want to remove.
3. Click **Purge Client events older than <specified> Year**.
4. Click OK.
Understanding the Symantec Endpoint Encryption administrative policies

This chapter includes the following topics:

- About administrative policies
- About types of administrative policies
- About install-time policies
- About Active Directory policies
- About native policies
- Differences between Active Directory policies and native policies
- About the Symantec Endpoint Encryption policy options
- About the Symantec Endpoint Encryption policy options available as install-time policies and as Active Directory or native policies
- About identifying the policy for a task

About administrative policies

Administrative policies are the policies that you, as a policy administrator, set using the Management Console for Management Agent, Drive Encryption,
Removable Media Encryption, Mac FileVault Client, and BitLocker Client. You configure these policies initially when you create the client installers. You can later use Active Directory policies or native policies to push policy updates to the clients.

About types of administrative policies

Symantec Endpoint Encryption provides the following types of policies that you create from the Management Console:

- Install-time policies
- Active Directory policies
- Native policies

About install-time policies

Install-time policies are the default policies set when you create the Management Agent, Drive Encryption or Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption client installers through the Management Console. You can modify an install-time policy by deploying the updated policy options that you defined using Active Directory or native policies. Active Directory and native policy settings take precedence over any installation settings on the client.

About Active Directory policies

Active Directory policies are known as Group Policy Objects (GPOs). They are designed for deployment to the computers that reside within your Active Directory forest or domain. You can create and deploy Active Directory policies whether synchronization with Active Directory is enabled or disabled.

About native policies

Native policies are designed for deployment to computers that Active Directory does not manage. If you want to deploy native policies to computers that Active Directory manages, turn off the synchronization with Active Directory.
Differences between Active Directory policies and native policies

Table 3-1 Differences between Active Directory policies and native policies

<table>
<thead>
<tr>
<th>Active Directory policies</th>
<th>Native policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies are applied in Local, Site, Domain, Organizational Unit (LSDOU) order of precedence.</td>
<td>Policies are applied in Computer, Subgroup, Group (CSG) order of precedence.</td>
</tr>
<tr>
<td>You can create or deploy an Active Directory policy through a single pane.</td>
<td>You have to click every pane to create a native policy.</td>
</tr>
<tr>
<td>Policies are obtained from the domain controller and applied at each restart.</td>
<td>Policies are applied when the client checks in with Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>An immediate policy update can be forced using the <code>gpupdate \force</code> or <code>secedit</code> command.</td>
<td>An immediate policy update can be forced when the user performs the following procedure:</td>
</tr>
<tr>
<td></td>
<td>1. Open the Symantec Endpoint Encryption Management Agent.</td>
</tr>
<tr>
<td></td>
<td>2. On the <strong>Internal Drives</strong> tab, click <strong>Status</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Check In</strong>.</td>
</tr>
</tbody>
</table>
About the Symantec Endpoint Encryption policy options

Table 3-2  Management Agent policy options

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
</table>
| Password Authentication | Configures the settings for the passwords that are used to authenticate to Symantec Endpoint Encryption and to encrypt or decrypt Removable Media Encryption files. The Password Authentication policy has the following options:  
  ■ Password Attempts—configures a logon delay in the Drive Encryption client to protect against Dictionary attack tools. For Drive Encryption, you can define the length of the delay for an invalid password attempt.  
  For Removable Media Encryption, by default a one-minute delay is active for failed file decryption attempts.  
  ■ Password Complexity—configures the minimum password length, uppercase and lowercase letters, digits, non-alphanumeric characters, and special characters that are allowed in a password. Only for the Removable Media Encryption clients.  
  ■ Maximum Password Age—defines a password expiration age, including the number of days in advance that a user should be warned. Only for the Removable Media Encryption clients.  
  ■ Password History—configures a restriction on password reuse, by defining the number of different passwords that users must use before they revert to old passwords. Only for the Removable Media Encryption clients.  
  See “Configuring the Management Agent - Password Authentication policy options” on page 113. |
| Communication           | Specifies the interval at which the recipient computers attempt to make contact with Symantec Endpoint Encryption Management Server.  
  See “Configuring the Management Agent - Communication policy options” on page 115. |
Table 3-3 Drive Encryption policy options

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
</table>
| Client Administrators | Provides the local support to Symantec Endpoint Encryption registered users. You create client administrators for Drive Encryption. Client administrators cannot change their own passwords or use any password-recovery methods. You can create a maximum of 1024 client administrators for each client installer package. Each client administrator account has the following privileges:  
  ■ User management—allows client administrators to register as well as unregister registered users  
  ■ Decrypt drives—provides client administrators with the right to decrypt disks encrypted using Drive Encryption  
  ■ Extend lockout—permits client administrators to extend a client computer’s next communication date, and  
  ■ Unlock—enables client administrators to unlock the client computers that have been locked for failure to communicate with Symantec Endpoint Encryption Management Server. Client administrators are always able to authenticate to client computers. Client administrators exercise these privileges using the Symantec Endpoint Encryption Drive Encryption Administrator Command Line.  
  See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.  
  See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.  
| Registered Users  | A registered user is one who is registered with Symantec Endpoint Encryption Drive Encryption. Only a registered user of Drive Encryption can access an encrypted disk. You can configure user registration to happen with or without a user’s intervention. At least one user must register with Symantec Endpoint Encryption on each Windows client computer. Symantec Endpoint Encryption supports the following three types of users:  
  1 Users authenticating using Windows credentials at preboot and at the Windows logon screen.  
  2 Users authenticating at preboot using Drive Encryption credentials, then authenticating to Windows using Windows credentials.  
  3 Users authenticating at preboot with a Windows user name and Drive Encryption password, then authenticating to Windows using Windows credentials. Users can authenticate to a Drive Encryption-encrypted disk using a password, a token, or both.  
  See “Configuring the Drive Encryption - Registered Users policy options” on page 122. |
<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Sign-On</td>
<td>Enables users to use their Windows credentials to authenticate at the Drive Encryption preboot login screen and then be automatically logged on to Windows. Users access the client computers without authenticating at the Windows logon screen. See “Configuring the Drive Encryption - Single Sign-On policy options” on page 125.</td>
</tr>
<tr>
<td>Self-Recovery</td>
<td>If a Drive Encryption user forgets their password, they can use Drive Encryption Self-Recovery to gain access to their computer without help desk assistance. The user bypasses the preboot authentication step by answering predefined security questions correctly. Drive Encryption Self-Recovery is not available to client administrators. See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.</td>
</tr>
</tbody>
</table>
| Startup        | Specifies the following features:  
  ■ A custom image or the Symantec Endpoint Encryption logo for the preboot startup screen. Alternatively, disable the startup screen.  
  ■ The text color for the legal notice that appears on the startup screen.  
  ■ The text for the legal notice that appears on the startup screen.  
  ■ A custom image or the Symantec Endpoint Encryption logo for the preboot login screen.  
  ■ The text color for the logon message that appears on the login screen.  
  ■ The logon customization details: You can enter a customized logon message. You can add this message using only when you create installation packages. You cannot use a GPO or native policy to update the logon message.  
  The custom image can be uploaded only when you create installation packages. The display option of the custom image can be enabled or disabled using a GPO or native policy. Once you generate an installer, you cannot provide a custom image through a GPO or native policy. To add or change a custom image, create a client installation package with the new image in it.  
  See “Configuring the Drive Encryption - Startup policy options” on page 126.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Logon History  | Specifies whether the Symantec Endpoint Encryption logon screen is prefilled with the user name, the domain, or both, of the last authenticated user.  
  **Note:** Using prefilled fields reduces the security of a client computer, so Symantec recommends deselecting both the **User name** and **Domain** check boxes.  
  **Note:** For a visually impaired user, uncheck **User name** and check **Domain**. This option combination allows the user to log on using audio cues. Use the Drive Encryption Administrator Command Line to enable the audio cue.  
  See “Configuring the Drive Encryption - Logon History policy options” on page 130.  
  See *Symantec Endpoint Encryption Drive Encryption Administrator Command Line Guide*.                                                                                                                                                                                                                                                                                                                                                                           |
<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Specifies the AES encryption strength, either 128 bit, or 256-bit. Drive Encryption uses the AES encryption strength to encrypt a client computer’s fixed disk. You can also specify whether you want to encrypt only the primary disk or all of the disks on client computers. An advanced Drive Encryption feature lets you specify double-writing sectors during encryption or decryption. Double-writing sectors during encryption or decryption guards against the remote possibility of losing a single data sector during power interruption. The power interruption must take place at the exact moment a disk sector is physically written. Selecting this option does not affect the performance of on-the-fly encryption and decryption. Power-loss protection is always enabled during fixed disk encryption and decryption. This option does not affect power-loss protection. If the computer is turned off or enters sleep or hibernation mode, the encryption or the decryption process continues automatically when power is restored. <strong>Note:</strong> You cannot use a GPO or native policy to update the install-time policy setting for encryption. See “Configuring the Drive Encryption - Encryption policy options” on page 130.</td>
</tr>
<tr>
<td>Client Monitor</td>
<td>Provides you with an option to enforce a client to communicate with Symantec Endpoint Encryption Management Server on a prescribed schedule. If a computer fails to connect to Symantec Endpoint Encryption Management Server, the users cannot authenticate to the computer. This feature ensures that the clients use the most recent policies on the Symantec Endpoint Encryption Management Server and update their latest reporting status to Symantec Endpoint Encryption Management Server. If the users are locked out of the computer at preboot authentication, only a client administrator or Help Desk Recovery can help regain access to the computer. See “Configuring the Drive Encryption - Client Monitor policy options” on page 131.</td>
</tr>
<tr>
<td>Policy</td>
<td>Options</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Help Desk Recovery  | In Symantec Endpoint Encryption versions earlier than 11.0, the Help Desk Recovery policy was known as the One-Time Password (OTP) policy. Help Desk Recovery makes use of a one-time password (also known as a Response Key). The help desk provides this key in the following cases:  
  ■ When a user forgets their password and cannot bypass the preboot authentication screen to access their computer.  
  ■ When a client computer fails to communicate with Symantec Endpoint Encryption Management Server within the schedule that a policy administrator prescribed, and a communication lockout is imminent.  
  Help Desk Recovery, therefore, provides an option to client users to recover their encrypted computer when they lack credentials to authenticate. Help Desk Recovery also allows them to authenticate when they are locked out at preboot.  
  Each computer has a unique one-time password that unlocks all the encrypted disks on that device. However when you apply a policy update, the policy is applied either to a user or to the computer, depending on the policy type. If the policy is an Active Directory policy, the enabled or disabled option applies to an individual user. If the policy is a native policy, the option applies to the computer, affecting all of those users.  
  See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 132. |
| Self-Encrypting Drives | Enables hardware encryption on Opal v2 compliant drives using an Opal drive’s built-in encryption capability.  
  See “Configuring the Drive Encryption - Self-Encrypting Drives policy options” on page 132.                                                                                                                   |
| Remote Decryption   | Remotely decrypts client computers. The computers remain decrypted, until this policy is reversed.  
  See “Configuring the Drive Encryption - Remote Decryption policy option” on page 134.                                                                                                                        |
Table 3-4 Removable Media Encryption policy options

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access and Encryption</td>
<td>Specifies the access and the encryption policy options that Removable Media Encryption enforces.</td>
</tr>
<tr>
<td></td>
<td>Access options include:</td>
</tr>
<tr>
<td></td>
<td>■ Do not allow access to files on removable media</td>
</tr>
<tr>
<td></td>
<td>■ Allow read-only access to files on removable media, or</td>
</tr>
<tr>
<td></td>
<td>■ Allow read and write access to files on removable media</td>
</tr>
<tr>
<td></td>
<td>Encryption options include:</td>
</tr>
<tr>
<td></td>
<td>■ Automatic encryption—Specifies automatic encryption of new files on removable media or automatic encryption of files according to Symantec Data Loss Prevention for Endpoint. You can also choose not to automatically encrypt the files on removable media.</td>
</tr>
<tr>
<td></td>
<td>■ On-demand encryption—Configures the computer to allow the users to selectively encrypt or decrypt individual files, groups of files, folders, or groups of folders. The users save these files and folders to removable media devices. You can configure the encrypt and decrypt features separately—for example the users can encrypt files on demand but not decrypt them, or conversely.</td>
</tr>
<tr>
<td>Device and File Type Exclusions</td>
<td>Specifies the removable storage devices and multimedia file types that should be excluded from automatic encryption on computers receiving this policy option.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Removable Media Encryption - Device and File Type Exclusions policy options” on page 139.</td>
</tr>
</tbody>
</table>
### Table 3-4  Removable Media Encryption policy options *(continued)*

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Method</td>
<td>Specifies the encryption methods that allow a Removable Media Encryption user to encrypt files. The users can use encryption methods of a password, a certificate, or both. These methods are available to:</td>
</tr>
<tr>
<td></td>
<td>■ The users who encrypt files and create self-decrypting archives from Removable Media Encryption–protected computers, and</td>
</tr>
<tr>
<td></td>
<td>■ The users who encrypt files using Removable Media Access Utility on the computers that Removable Media Encryption does not protect.</td>
</tr>
<tr>
<td></td>
<td>For more information on how the users encrypt a file using a password, a certificate, or both, see the <em>Symantec Endpoint Encryption Client Online Help</em>.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Removable Media Encryption - Encryption Method policy options” on page 140.</td>
</tr>
</tbody>
</table>
Removable Media Encryption uses default passwords to reduce the number of prompts users receive when they encrypt or decrypt files and folders. Once a user sets a default password, that password is used for encryption. If an existing file or folder was encrypted to the default password, the file is decrypted without prompting the user for credentials. You can let users set one default password, plus up to two session passwords. Alternatively, you can let users set a device session password, which is useful in a kiosk environment.

If you do not allow users to set default passwords, they are prompted to enter a password each time they encrypt or decrypt a file.

You can apply password aging to default passwords and to session passwords, to ensure that users define passwords that conform to restrictions you define. These restrictions include a maximum password age and a limit on password reuse. You define them using the Management Agent Password Authentication policy. For session passwords, you can alternatively define expiration methods of deletion or deactivation at the end of Windows sessions.

**Note:** If the encryption method is certificates only, then default passwords are not used.

**Note:** For the Symantec Endpoint Encryption Management Server version 11.x release, the Default Password setting is enabled by default when you create an install-time policy. For upgrades from a previous version of Symantec Endpoint Encryption Management Server to version 11.x, the Default Passwords page appears as an Active Directory or native policy.

### Table 3-4
Removable Media Encryption policy options (continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Passwords</td>
<td>Removable Media Encryption uses default passwords to reduce the number of prompts users receive when they encrypt or decrypt files and folders. Once a user sets a default password, that password is used for encryption. If an existing file or folder was encrypted to the default password, the file is decrypted without prompting the user for credentials. You can let users set one default password, plus up to two session passwords. Alternatively, you can let users set a device session password, which is useful in a kiosk environment. If you do not allow users to set default passwords, they are prompted to enter a password each time they encrypt or decrypt a file. You can apply password aging to default passwords and to session passwords, to ensure that users define passwords that conform to restrictions you define. These restrictions include a maximum password age and a limit on password reuse. You define them using the Management Agent Password Authentication policy. For session passwords, you can alternatively define expiration methods of deletion or deactivation at the end of Windows sessions. <strong>Note:</strong> If the encryption method is certificates only, then default passwords are not used. <strong>Note:</strong> For the Symantec Endpoint Encryption Management Server version 11.x release, the Default Password setting is enabled by default when you create an install-time policy. For upgrades from a previous version of Symantec Endpoint Encryption Management Server to version 11.x, the Default Passwords page appears as an Active Directory or native policy.</td>
</tr>
</tbody>
</table>
### Removable Media Encryption policy options *(continued)*

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Certificate</td>
<td>This policy applies only to computers on which write access and encryption are enabled for removable media encryption devices. You enable these options through the Access and Encryption policy. When the user-provided credentials are not available, a recovery certificate is used to decrypt encrypted files. A master certificate can be used as a recovery certificate for Removable Media Encryption that allows users to recover from forgotten passwords and lost certificates. The public key of the master certificate is used as an additional key to encrypt the files that the users encrypt with Removable Media Encryption. Therefore, an administrator can decrypt and recover files if a user forgets their password or loses their certificate. The administrator can decrypt using the recovery certificate even if it has expired. You need two copies of the same recovery certificate, one with the private key and one without. <strong>Without the private key</strong> - the recovery certificate is deployed to clients using an installation package or a policy. Upon receipt, clients encrypt files using the recovery certificate in addition to the credentials that the user provides. <strong>With the private key</strong> - the recovery certificate is exported using the .pfx format. It should be stored in a safe, physically secure location. Symantec recommends exporting it to a token or a smart card and then securing the token or the smart card in a fire-proof vault. See “Configuring the Removable Media Encryption - Recovery Certificate policy options” on page 142.</td>
</tr>
</tbody>
</table>
### Table 3-4 Removable Media Encryption policy options (continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portability</td>
<td>Specifies whether to automatically copy Removable Media Access Utility to removable media and to allow users to create self-decrypting archives. Removable Media Access Utility is available for the Windows operating system as well as the Mac OS X operating system.</td>
</tr>
<tr>
<td></td>
<td>■ Access Utility—Removable Media Access Utility lets you encrypt and decrypt files on the computers that Removable Media Encryption does not protect. Removable Media Access Utility also lets you decrypt files encrypted using Symantec Endpoint Encryption Removable Storage versions earlier than Symantec Endpoint Encryption version 11.0. Removable Media Access Utility is available for the Windows operating system as well as the Mac OS X operating system. If a device is exempted from encryption, Removable Media Access Utility is not written to that device. You define exemptions using the Device and File Type Exclusions policy.</td>
</tr>
<tr>
<td></td>
<td>■ Self-Decrypting Archive—Allows the users to create encrypted self-decrypting archive files for secure transport. Self-decrypting archive files can be decrypted from any computer, without any need for Removable Media Encryption or Removable Media Access Utility. In Symantec Endpoint Encryption version 11.0, only password encrypted self-decrypting archive is supported. Certificates are not supported for a self-decrypting archive. For more information on Removable Media Access Utility, see the <a href="#">Removable Media Access Utility Help</a>. For more information on self-decrypting archives, see the <a href="#">Self-Decrypting Archive Online Help</a>. See “Configuring the Removable Media Encryption - Portability policy options” on page 144.</td>
</tr>
</tbody>
</table>
| Expired Certificates | For Removable Media Encryption, with the expired certificates policy option, the users can encrypt their files with expired certificates.  

See “Configuring the Removable Media Encryption - Expired Certificates policy options” on page 145.
### Table 3-4  Removable Media Encryption policy options (continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workgroup Key</td>
<td>Removable Media Encryption and Removable Media Access Utility use the workgroup key to encrypt files—in addition to the user-provided passwords, certificate(s), or both. The workgroup key facilitates the sharing of encrypted files among users within a group. For example, a workgroup key on the Removable Media Encryption–protected computer matches the workgroup key with which a file was encrypted. The user is not prompted to provide a password or certificate to decrypt that file.</td>
</tr>
</tbody>
</table>

### Table 3-5  Mac FileVault Client policy options

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>Lists the version numbers of the Apple Mac OS X operating systems for which you can create the Symantec Endpoint Encryption for FileVault client installation package. See “Configuring the Mac FileVault Client - Introduction policy options” on page 147.</td>
</tr>
<tr>
<td>Institutional Recovery Key</td>
<td>Specifies whether you want to include an Institutional Recovery Key certificate in the install-time policy while you create the Symantec Endpoint Encryption for FileVault client installation package. See “Configuring the Mac FileVault Client - Institutional Recovery Key policy options” on page 148.</td>
</tr>
<tr>
<td>Communication</td>
<td>Specifies the interval at which the recipient Macintosh computers that have Symantec Endpoint Encryption for FileVault installed attempt to make contact with Symantec Endpoint Encryption Management Server. See “Configuring the Mac FileVault Client - Communication policy options” on page 149.</td>
</tr>
</tbody>
</table>
Table 3-6  BitLocker Client policy options

<table>
<thead>
<tr>
<th>Policy</th>
<th>Options</th>
</tr>
</thead>
</table>
| Encryption and Authentication | Encryption - Specifies the XTS-AES or AES encryption strength. BitLocker encryption uses the XTS-AES or AES encryption strength to encrypt a client computer's boot volume as well as the data volumes.  
Note: The XTS-AES encryption mode for BitLocker is only available in systems with Windows 10 version 1511 and later installed. Alternatively, for systems with Windows 10 version 1511 earlier installed, AES encryption mode is available.  
Authentication - Specifies the authentication methods that are available so that users can gain access to the client computer using a TPM or a TPM and a PIN. The users authenticate with a password for the client computers that do not support TPM.  
Decryption - Specifies that decryption policy option allows you to decrypt all the volumes on a client computer that has Symantec Endpoint Encryption for BitLocker installed.  
See “Configuring the BitLocker Client - Encryption and Authentication policy options” on page 150. |
| Client Monitor               | Provides you with an option to enforce a client encrypted with Symantec Endpoint Encryption for BitLocker to communicate with Symantec Endpoint Encryption Management Server on a prescribed time interval. If a computer fails to connect to Symantec Endpoint Encryption Management Server, the computer is locked out. This feature ensures that the clients use the most recent policies on the server and update their latest reporting status to the server. If the computer is locked out, only Help Desk Recovery can help regain access to the computer.  
See “Configuring the BitLocker Client - Client Monitor policy options” on page 151. |

About using best practices for client lockout

You can set a client lockout policy for Drive Encryption or for BitLocker Client using the Client Monitor policy. This policy allows you to enforce a prescribed minimum contact period within which clients must check in with the Symantec Endpoint Encryption Management Server. Users are warned if a lockout is near. If clients do not check in within the prescribed period, the client is locked.

If you are using the client lockout feature, as a best practice, set a BIOS password to prevent users from changing BIOS settings. This restricts users from making
changes to the System Date in an attempt to circumvent this feature. If a user changes the date and:

- If the client is already in a locked state, the client remains locked. The date change has no effect.
- If the client is in a warning state and is rebooted, the client launches normally, without issuing a warning message. If the client exceeds the communication limit, the client is locked without warning.
- If the client is in a warning state or normal period, the Windows Time Service eventually re-syncs the client date/time to match the enterprise domain or internet time servers.

Therefore, the user cannot circumvent this feature and if they try to, they can put themselves in a situation where their system is locked without warning.

About the Symantec Endpoint Encryption policy options available as install-time policies and as Active Directory or native policies

The table lists the Symantec Endpoint Encryption policies available as install-time policies and as Active Directory or native policies. The policies are listed in the order in which they appear in the installation wizards.

Table 3-7 Available policy options for install-time policies and Active Directory (GPO) or native policies

<table>
<thead>
<tr>
<th>Feature</th>
<th>Policy title</th>
<th>Install-time policy</th>
<th>Active Directory (GPO) or native policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Agent</td>
<td>Password Authentication</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Communication</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>Drive Encryption</td>
<td>Client Administrators</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Registered Users</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Single Sign-On</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Self-Recovery</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Startup</td>
<td>y</td>
<td>y</td>
</tr>
</tbody>
</table>
Understanding the Symantec Endpoint Encryption administrative policies

About the Symantec Endpoint Encryption policy options available as install-time policies and as Active Directory or native policies

Table 3-7

<table>
<thead>
<tr>
<th>Feature</th>
<th>Policy title</th>
<th>Install-time policy</th>
<th>Active Directory (GPO) or native policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logon History</td>
<td></td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td>y</td>
<td>n/a</td>
</tr>
<tr>
<td>Client Monitor</td>
<td></td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>Help Desk Recovery</td>
<td></td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>Self-Encrypting Drives</td>
<td></td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td>Windows Password Reset</td>
<td></td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>Remote Decryption</td>
<td></td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>Removable Media Encryption</td>
<td>Access and Encryption</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Device and File Type Exclusions</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Encryption Method</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Default Passwords</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Recovery Certificate</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Portability</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Expired Certificates</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Workgroup Key</td>
<td>n/a</td>
<td>y</td>
</tr>
<tr>
<td>Mac FileVault Client</td>
<td>Introduction</td>
<td>y</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>Institutional Recovery Key</td>
<td>y</td>
<td>n/a</td>
</tr>
<tr>
<td>BitLocker Client</td>
<td>Communication</td>
<td>y</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>Encryption and Authentication</td>
<td>y</td>
<td>y</td>
</tr>
<tr>
<td></td>
<td>Client Monitor</td>
<td>y</td>
<td>y</td>
</tr>
</tbody>
</table>
About identifying the policy for a task

Use the table to look up the administrative tasks by policy name.

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive Encryption policies and tasks:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Administrators</td>
<td>Add a client administrator account</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.</td>
</tr>
<tr>
<td></td>
<td>Change a client administrator account</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.</td>
</tr>
<tr>
<td></td>
<td>Delete a client administrator account</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.</td>
</tr>
<tr>
<td></td>
<td>Load the list of existing client administrator accounts</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.</td>
</tr>
<tr>
<td>Client Monitor</td>
<td>Force a client computer to check in with the server</td>
<td>See “Configuring the Drive Encryption - Client Monitor policy options” on page 131.</td>
</tr>
<tr>
<td></td>
<td>Define a minimum check-in period for client computers, as well as a warning period for computers about to be locked out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lock the computers that do not check in with the server</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-8 Administrative tasks, by policy (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Define the encryption strength</td>
<td>See “Configuring the Drive Encryption - Encryption policy options” on page 130.</td>
</tr>
<tr>
<td></td>
<td>Choose whether only one disk or all disks are encrypted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Choose to double-write sectors during encryption and decryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Choose to include or skip the encryption of unused disk space on the client computer</td>
<td></td>
</tr>
<tr>
<td>Help Desk Recovery</td>
<td>Set a one-time password recovery option</td>
<td>See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 132.</td>
</tr>
<tr>
<td></td>
<td>Allow the Help Desk Recovery option to unlock a locked computer</td>
<td></td>
</tr>
<tr>
<td>Logon History</td>
<td>Prefill the pre-Windows authentication screen with the most recent user name</td>
<td>See “Configuring the Drive Encryption - Logon History policy options” on page 130.</td>
</tr>
<tr>
<td></td>
<td>Prefill the pre-Windows authentication screen with the most recent domain</td>
<td></td>
</tr>
<tr>
<td>Registered Users</td>
<td>Define or change a registered user's authentication method to be password, token, or both</td>
<td>See “Configuring the Drive Encryption - Registered Users policy options” on page 122.</td>
</tr>
<tr>
<td>Startup</td>
<td>Define or reinstate the logo at startup to be either the default Symantec Endpoint Encryption logo or a custom image</td>
<td>See “Configuring the Drive Encryption - Startup policy options” on page 126.</td>
</tr>
</tbody>
</table>
Table 3-8  Administrative tasks, by policy *(continued)*

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define the legal notice at startup to be either the default Symantec Endpoint Encryption message or a custom message</td>
<td>See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.</td>
<td></td>
</tr>
<tr>
<td>Define the logon message at startup to be either the default Symantec Endpoint Encryption message or a custom message</td>
<td>See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.</td>
<td></td>
</tr>
<tr>
<td>Configure the color of the legal notice text and the logon message text</td>
<td>See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.</td>
<td></td>
</tr>
<tr>
<td>Self-Recovery</td>
<td>Enable or disable the Drive Encryption Self-Recovery method</td>
<td>See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.</td>
</tr>
<tr>
<td>Define or change the number of predefined questions or the number of user-defined questions. Create or change the content of any predefined questions or the minimum answer length required.</td>
<td>See “Configuring the Drive Encryption - Single Sign-On policy options” on page 125.</td>
<td></td>
</tr>
<tr>
<td>Enable or disable the Single Sign-On option</td>
<td>See “Configuring the Drive Encryption - Single Sign-On policy options” on page 125.</td>
<td></td>
</tr>
<tr>
<td>Enables or disables hardware encryption on Opal v2 compliant drives using an Opal drive’s built-in encryption capability.</td>
<td>See “Configuring the Drive Encryption - Self-Encrypting Drives policy options” on page 132.</td>
<td></td>
</tr>
<tr>
<td>Enables or disables the Windows Password Reset feature on Drive Encryption client computers.</td>
<td>See “Configuring the Drive Encryption - Windows Password Reset policy option” on page 133.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3-8  Administrative tasks, by policy *(continued)*

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Decryption</td>
<td>Allows for the remote decryption of all disks and partitions on client computers. A computer remains in a decrypted state, until this policy is reversed.</td>
<td>See “Configuring the Drive Encryption - Remote Decryption policy option” on page 134.</td>
</tr>
</tbody>
</table>

Removable Media Encryption policies and tasks:

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access and Encryption</td>
<td>Define or change any read or write access permissions that are allowed to removable media, if any.</td>
<td>See “Configuring the Removable Media Encryption - Access and Encryption policy options” on page 135.</td>
</tr>
<tr>
<td></td>
<td>Set the encryption format to be the version 11.x format, or the version 8.2.1 format for backward compatibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Define or change the extent of automatic encryption, if any.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Automatic encryption of files according to the Symantec Data Loss Prevention product can be enabled only if the Data Loss Prevention software is installed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enable or disable whether users can use a menu option to encrypt a file, or to decrypt a file, or both</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allow users to choose the automatic encryption behavior to be to encrypt or not to encrypt</td>
<td></td>
</tr>
<tr>
<td>Policy name</td>
<td>Task</td>
<td>Policy URL</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default Passwords</td>
<td>Allow users to set a default password and up to two session passwords. Password aging, which can include password history, can be applied. Alternatively, users can set a device session password for each device.</td>
<td>See “Configuring the Removable Media Encryption - Default Passwords policy options” on page 140.</td>
</tr>
<tr>
<td>Device and File Type Exclusions</td>
<td>Exclude multimedia files from automatic encryption. Choose from audio, video, and image.</td>
<td>See “Configuring the Removable Media Encryption - Device and File Type Exclusions policy options” on page 139.</td>
</tr>
<tr>
<td></td>
<td>Exclude file types from automatic encryption by file extension</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exclude up to 50 multimedia devices from encryption by vendor (and optionally, by product ID)</td>
<td></td>
</tr>
<tr>
<td>Encryption Method</td>
<td>Choose the encryption method to be password, certificate, or both</td>
<td>See “Configuring the Removable Media Encryption - Encryption Method policy options” on page 140.</td>
</tr>
<tr>
<td>Expired Certificates</td>
<td>Enable or disable users from encrypting files with expired certificates</td>
<td>See “Configuring the Removable Media Encryption - Expired Certificates policy options” on page 145.</td>
</tr>
<tr>
<td>Portability</td>
<td>Allow the Removable Media Access Utility to be copied to removable devices, to enable encryption and decryption of files on computers not running Removable Media Encryption. Select a Windows version, a Mac OS X version, or both.</td>
<td>See “Configuring the Removable Media Encryption - Portability policy options” on page 144.</td>
</tr>
</tbody>
</table>
Table 3-8 Administrative tasks, by policy (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow users to save files as self-decrypting archives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recovery Certificate</td>
<td>Allow files to be encrypted also with a recovery certificate. Select or change the certificate.</td>
<td>See “Configuring the Removable Media Encryption - Recovery Certificate policy options” on page 142.</td>
</tr>
<tr>
<td>Workgroup Key</td>
<td>Enable or disable the use of a workgroup key for encryption, for easier file sharing. The key is random; generate it within the policy or copy and paste it into the policy.</td>
<td>See “Configuring the Removable Media Encryption - Workgroup Key policy options” on page 145.</td>
</tr>
<tr>
<td>Management Agent policies and tasks:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication</td>
<td>Define or change the frequency with which client computers send status updates to the Management Server.</td>
<td>See “Configuring the Management Agent - Communication policy options” on page 115.</td>
</tr>
<tr>
<td></td>
<td>Define the Management Server communication credentials.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3-8  Administrative tasks, by policy (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Authentication</td>
<td>Define or change the password settings that are related to registered users authentication attempts and password complexity. For preboot authentication, define the number of password attempts that are allowed before a defined pause is enforced between further attempts. For Removable Media Encryption, define the number of password attempts allowed to provide a decryption password, before a one-minute pause is enforced between further attempts. For Removable Media Encryption, define the complexity requirements for encryption passwords, by defining the amount and type of characters and digits required. Also define any Password Aging and Password History requirements. In Drive Encryption, the preboot authentication password is the Windows password, which is used for single sign-on.</td>
<td>See “Configuring the Management Agent - Password Authentication policy options” on page 113.</td>
</tr>
</tbody>
</table>

Mac FileVault Client policies and tasks:
### Table 3-8  Administrative tasks, by policy (continued)

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Institutional Recovery Key</strong></td>
<td>Choose to include an Institutional Recovery Key certificate in the install-time policy when you create the Symantec Endpoint Encryption for FileVault package.</td>
<td>See “Configuring the Mac FileVault Client - Institutional Recovery Key policy options” on page 148.</td>
</tr>
<tr>
<td><strong>Communication</strong></td>
<td>Define or change the frequency with which Macintosh client computers send status updates to the Management Server.</td>
<td>See “Configuring the Mac FileVault Client - Communication policy options” on page 149.</td>
</tr>
<tr>
<td></td>
<td>Define the Management Server communication credentials.</td>
<td></td>
</tr>
<tr>
<td><strong>BitLocker Client policies and tasks:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td>Define the encryption strength to encrypt the boot and the data volumes using Symantec Endpoint Encryption for BitLocker.</td>
<td>See “Configuring the BitLocker Client - Encryption and Authentication policy options” on page 150.</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Define or change a Symantec Endpoint Encryption for BitLocker client users authentication method to be TPM, TPM and PIN, or password.</td>
<td>See “Configuring the BitLocker Client - Encryption and Authentication policy options” on page 150.</td>
</tr>
<tr>
<td><strong>Client Monitor</strong></td>
<td>Force a client computer encrypted with Symantec Endpoint Encryption for BitLocker to check in with the server</td>
<td>See “Configuring the BitLocker Client - Client Monitor policy options” on page 151.</td>
</tr>
</tbody>
</table>
Table 3-8  Administrative tasks, by policy *(continued)*

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Task</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Define a minimum check-in period for client computers, as well as a warning period for computers about to be locked out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lock the computers that do not check in with the server within the defined time frame.</td>
<td></td>
</tr>
</tbody>
</table>

Use the table to look up the policy that is related to an administrative task.

Table 3-9  Administrative tasks, with policy reference

<table>
<thead>
<tr>
<th>Task</th>
<th>Policy name</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive Encryption tasks and policies:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add a client administrator account</td>
<td>Client Administrators</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.</td>
</tr>
<tr>
<td>Change a client administrator account</td>
<td>Client Administrators</td>
<td></td>
</tr>
<tr>
<td>Decrypt a computer remotely</td>
<td>Remote Decryption</td>
<td>See “Configuring the Drive Encryption - Remote Decryption policy option” on page 134.</td>
</tr>
<tr>
<td>Define the encryption strength</td>
<td>Encryption</td>
<td>See “Configuring the Drive Encryption - Encryption policy options” on page 130.</td>
</tr>
<tr>
<td>Delete a client administrator account</td>
<td>Client Administrators</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.</td>
</tr>
<tr>
<td>Task</td>
<td>Policy name</td>
<td>Policy URL</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Double-write sectors during drive encryption and decryption</td>
<td>Encryption</td>
<td>See “Configuring the Drive Encryption - Encryption policy options” on page 130.</td>
</tr>
<tr>
<td>Enable or disable the Self-Recovery password recovery method. Includes the options to:</td>
<td>Self-Recovery</td>
<td>See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.</td>
</tr>
<tr>
<td>■ Define or change the number of predefined questions or the number of user-defined questions.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Create or change the content of any predefined question or the minimum answer length required.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enable the Help Desk Recovery option</td>
<td>Help Desk Recovery (formerly OTP)</td>
<td>See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 125.</td>
</tr>
<tr>
<td>Enable or disable hardware encryption on Opal v2 compliant drives using an Opal drive's built-in encryption capability.</td>
<td>Self-Encrypting Drives</td>
<td>See “Configuring the Drive Encryption - Self-Encrypting Drives policy options” on page 132.</td>
</tr>
<tr>
<td>Force a client computer to check in with the server</td>
<td>Client Monitor</td>
<td>See “Configuring the Drive Encryption - Client Monitor policy options” on page 131.</td>
</tr>
<tr>
<td>Task</td>
<td>Policy name</td>
<td>Policy URL</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Load the list of existing client administrator accounts into the panel to add, change, or delete client administrators</td>
<td>Client Administrators</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117. See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.</td>
</tr>
<tr>
<td>Lock the computers that do not check in with the server</td>
<td>Client Monitor</td>
<td>See “Configuring the Drive Encryption - Client Monitor policy options” on page 131.</td>
</tr>
<tr>
<td>Prefill the preboot authentication screen with the most recent:</td>
<td>Logon History</td>
<td>See “Configuring the Drive Encryption - Logon History policy options” on page 130.</td>
</tr>
<tr>
<td>■ Domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ User name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set a minimum check-in period for client computers, as well as a warning period for any computers that are about to be locked</td>
<td>Client Monitor</td>
<td>See “Configuring the Drive Encryption - Client Monitor policy options” on page 131.</td>
</tr>
<tr>
<td>Set or change a registered user’s authentication method to be password, token, or both</td>
<td>Registered User</td>
<td>See “Configuring the Drive Encryption - Registered Users policy options” on page 122.</td>
</tr>
<tr>
<td>Set or reinstate the startup logo to be either the default Symantec Endpoint Encryption logo or a custom image</td>
<td>Startup</td>
<td>See “Configuring the Drive Encryption - Startup policy options” on page 126.</td>
</tr>
<tr>
<td>Set the startup logon message to be either the default Symantec Endpoint Encryption message or a custom message</td>
<td>Startup</td>
<td></td>
</tr>
</tbody>
</table>
### Table 3-9

Administrative tasks, with policy reference *(continued)*

<table>
<thead>
<tr>
<th>Task</th>
<th>Policy name</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlock a locked computer using the Help Desk Recovery option</td>
<td>Help Desk Recovery</td>
<td>See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 132.</td>
</tr>
</tbody>
</table>

Removable Media Encryption tasks and policies:

<table>
<thead>
<tr>
<th>Task</th>
<th>Policy name</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow files to be encrypted also with a recovery certificate</td>
<td>Recovery Certificate</td>
<td>See “Configuring the Removable Media Encryption - Recovery Certificate policy options” on page 142.</td>
</tr>
<tr>
<td>Allow the Removable Media Access Utility to be copied to removable devices</td>
<td>Portability</td>
<td>See “Configuring the Removable Media Encryption - Portability policy options” on page 144.</td>
</tr>
<tr>
<td>Allow users to choose the automatic encryption behavior</td>
<td>Access and Encryption</td>
<td>See “Configuring the Removable Media Encryption - Access and Encryption policy options” on page 135.</td>
</tr>
<tr>
<td>Allow users to encrypt files as self-decrypting archives</td>
<td>Portability</td>
<td>See “Configuring the Removable Media Encryption - Portability policy options” on page 144.</td>
</tr>
<tr>
<td>Allow users to set default passwords for encryption. Default passwords include one default password plus up to two session passwords, or a device session password.</td>
<td>Default Passwords</td>
<td>See “Configuring the Removable Media Encryption - Default Passwords policy options” on page 140.</td>
</tr>
<tr>
<td>Apply password aging, which can include password history</td>
<td>Default Passwords</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>Policy name</td>
<td>Policy URL</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Choose the encryption method to be password, certificate, or both</td>
<td>Encryption Method</td>
<td>See “Configuring the Removable Media Encryption - Encryption Method policy options” on page 140.</td>
</tr>
<tr>
<td>Define or change the extent of automatic encryption, if any</td>
<td>Access and Encryption</td>
<td>See “Configuring the Removable Media Encryption - Access and Encryption policy options” on page 135.</td>
</tr>
<tr>
<td>Define the encryption format for files encrypted to removable media.</td>
<td>Access and Encryption</td>
<td>Choices are the version 11.x format or the version 8.2.1 backward-compatible format</td>
</tr>
<tr>
<td>Define or change any read or write access permissions that are allowed to removable media, if any</td>
<td>Access and Encryption</td>
<td></td>
</tr>
<tr>
<td>Enable or disable the use of a workgroup key for encryption, for easier file sharing</td>
<td>Workgroup Key</td>
<td>See “Configuring the Removable Media Encryption - Workgroup Key policy options” on page 145.</td>
</tr>
<tr>
<td>Enable or disable users from encrypting files with expired certificates</td>
<td>Expired Certificates</td>
<td>See “Configuring the Removable Media Encryption - Expired Certificates policy options” on page 145.</td>
</tr>
<tr>
<td>Enable or disable whether users can use a menu option to encrypt a file, or to decrypt a file, or both</td>
<td>Access and Encryption</td>
<td>See “Configuring the Removable Media Encryption - Access and Encryption policy options” on page 135.</td>
</tr>
</tbody>
</table>
About identifying the policy for a task

Table 3-9  Administrative tasks, with policy reference (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Policy name</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exclude file types from automatic encryption by file extension</td>
<td>Device and File Type Exclusions</td>
<td>See “Configuring the Removable Media Encryption - Device and File Type Exclusions policy options” on page 139.</td>
</tr>
<tr>
<td>Exclude multimedia devices from encryption by vendor (and optionally by product ID)</td>
<td>Device and File Type Exclusions</td>
<td></td>
</tr>
<tr>
<td>Exclude multimedia files from automatic encryption</td>
<td>Device and File Type Exclusions</td>
<td></td>
</tr>
</tbody>
</table>

Management Agent tasks and policies:

<table>
<thead>
<tr>
<th>Task</th>
<th>Policy name</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define or change the frequency with which client computers send status updates to the Management Server</td>
<td>Communication</td>
<td>See “Configuring the Management Agent - Communication policy options” on page 115.</td>
</tr>
<tr>
<td>Define or change password settings: complexity, maximum age, and history requirements</td>
<td>Password Authentication</td>
<td>See “Configuring the Management Agent - Password Authentication policy options” on page 113.</td>
</tr>
<tr>
<td>Define the Management Server communication credentials</td>
<td>Communication</td>
<td>See “Configuring the Management Agent - Communication policy options” on page 115.</td>
</tr>
</tbody>
</table>

Mac FileVault Client tasks and policies:

<table>
<thead>
<tr>
<th>Task</th>
<th>Policy name</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define or change the frequency with which Macintosh client computers send status updates to the Management Server</td>
<td>Communication</td>
<td>See “Configuring the Mac FileVault Client - Communication policy options” on page 149.</td>
</tr>
</tbody>
</table>
### Table 3-9

<table>
<thead>
<tr>
<th>Task</th>
<th>Policy name</th>
<th>Policy URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose to include an Institutional Recovery Key certificate in the</td>
<td>Institutional Recovery Key</td>
<td>See “Configuring the Mac FileVault Client - Institutional Recovery Key policy options” on page 148.</td>
</tr>
<tr>
<td>install-time policy for recovery of the Symantec Endpoint Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>for FileVault users</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define the Management Server communication credentials</td>
<td>Communication</td>
<td>See “Configuring the Mac FileVault Client - Communication policy options” on page 149.</td>
</tr>
<tr>
<td>BitLocker Client tasks and policies:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define the encryption strength for encrypting the volumes using</td>
<td>Encryption and Authentication</td>
<td>See “Configuring the BitLocker Client - Encryption and Authentication policy options” on page 150.</td>
</tr>
<tr>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set or change a Symantec Endpoint Encryption for BitLocker user’s</td>
<td>Encryption and Authentication</td>
<td>See “Configuring the BitLocker Client - Encryption and Authentication policy options” on page 150.</td>
</tr>
<tr>
<td>authentication method to be TPM, TPM and PIN, or password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set a minimum check-in period for the client computers encrypted</td>
<td>Client Monitor</td>
<td>See “Configuring the BitLocker Client - Client Monitor policy options” on page 151.</td>
</tr>
<tr>
<td>with Symantec Endpoint Encryption for BitLocker, as well as a warning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>period for any computers that are about to be locked</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Creating Symantec Endpoint Encryption client installers

This chapter includes the following topics:

■ About client installers
■ About the installation settings wizards
■ Creating a Symantec Endpoint Encryption Client installation package
■ About enabling features in the Symantec Endpoint Encryption Client installation package
■ Creating a Symantec Endpoint Encryption for FileVault installation package
■ Creating a Windows Password Reset Utility installation package

About client installers

Purpose

The Symantec Endpoint Encryption client installation packages deliver the client software and initial settings to the client computers. For the Microsoft Windows client computers, the installation package contains Management Agent, either Drive Encryption or Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption. For the Macintosh client computers, the installation package contains Symantec Endpoint Encryption for FileVault.
**Note:** The Symantec Endpoint Encryption Client installation package also installs the Symantec Endpoint Encryption Client Administrator Console.

You create the Symantec Endpoint Encryption client installation packages from the Management Console.

**Client installer package contents**

The client installation packages consist of the following installers, and log files for Management Agent and the Drive Encryption or Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption features. Each log file documents the feature-specific contents of the installer and includes the file name and the date and time that the installer was created.

- BitLockerSettings month_day_year-hour.minute.sec.log
- DriveEncryptionSettings month_day_year-hour.minute.sec.log
- ManagementAgentSettings month_day_year-hour.minute.sec.log
- RemovableMediaEncryptionSettings month_day_year-hour.minute.sec.log
- SEE Client.msi
- SEE Client_x64.msi
- SEEInstaller.zip

**Note:** The SEEInstaller.zip folder is created to install Symantec Endpoint Encryption for FileVault on the Macintosh computers. The compressed folder consists of the SEEInstaller-<version number of the release>.<build number>.pkg and MacSettings.xml files.

**Note:** Dual management console functionality requires at least Symantec Endpoint Encryption 8.2.1 MP14: If you use Symantec Endpoint Encryption 11.1.2 with dual management consoles, your 8.2.1 environment requires at least Symantec Endpoint Encryption 8.2.1 MP14 if you want to generate MSIs for SEE Full Disk or SEE Removable Storage clients.

---

**About the installation settings wizards**

You can create the Symantec Endpoint Encryption Client installation package by running the Windows Client installation settings wizard from the Management Console. The wizard enables you to define policy settings for the following features:
You can create the Symantec Endpoint Encryption for FileVault installation package by running the Symantec Endpoint Encryption for FileVault installation settings wizard from the Management Console.

**Note:** The Symantec Endpoint Encryption for FileVault installation package does not change any policy settings. The client installation package identifies the client computers to the Symantec Endpoint Encryption Management Server for tracking and reporting purposes and for computer access recovery. Policy settings are defined using a GPO only.

On the final page of each wizard, you are prompted for a location to save the client installation settings MSI package.

For Symantec Endpoint Encryption Client, two MSI packages are saved, for 32- and 64-bit Windows editions. The 64-bit package is appended with _x64.

For Symantec Endpoint Encryption for FileVault, shown in the Management Console user interface as **Mac FileVault Client**, the MSI package is saved as a .zip folder. The SEEInstaller.zip folder consists of the SEEInstaller-<version number of the release>.-<build number>.pkg and MacSettings.xml files.

Save the package in a shared network location, such as the SYSVOL folder on the domain controller.

You cannot load a previously created client installation package to examine the settings. You can know the contents of each MSI, however, in two ways:

- Save each client installer package with a descriptive name. A descriptive name is helpful if you plan to deploy multiple sets of packages throughout your organization.

- View the log files that Symantec Endpoint Encryption creates with each MSI. The individual settings that you selected for a given feature are saved in a date- and time-stamped log file. An example of a log file name is “ManagementAgentSettings 3_27_2014-18.21.59.log.”

The log file is created in the same location that you specified when you saved the package.
The log file does not show the contents of password fields. You should separately record and store in a secure location all passwords that you specify in an installation package.

Creating a Symantec Endpoint Encryption Client installation package

The Windows Client Installation Settings wizard walks you through a series of panels, where you choose the features that you want to include in the Symantec Endpoint Encryption Client installation package. Then, you configure the initial policy settings that are applied when Symantec Endpoint Encryption Client is installed.

See “About enabling features in the Symantec Endpoint Encryption Client installation package” on page 93.

Note: The Symantec Endpoint Encryption Client installation package always installs Management Agent. If you choose to include the Drive Encryption feature in the Symantec Endpoint Encryption Client installation package, the package also installs the Symantec Endpoint Encryption Client Administrator Console and the Administrator Command Line without any additional policy configuration.

Perform the following procedure to create an Symantec Endpoint Encryption Client installation package.

To create an Symantec Endpoint Encryption Client installation package

1. In the left pane, click Symantec Endpoint Encryption Software Setup > Windows Client.

2. On the Windows Client Installation Settings – Features page, select the features that you want to enable in the Symantec Endpoint Encryption Client installation package. Some features might not be available for selection depending upon whether they were disabled during the Symantec Endpoint Encryption Management Server installation.

Note: For the Disk encryption option, you can select either the Drive Encryption feature, or Symantec Endpoint Encryption for BitLocker. If you select Drive Encryption, ensure that the Microsoft BitLocker feature is disabled on the Microsoft Windows computers on which you want to install Symantec Endpoint Encryption Client. If you select Symantec Endpoint Encryption for BitLocker, ensure that you install Symantec Endpoint Encryption Client on Windows computers that support the BitLocker feature.
3 Click **Next**.

4 On the **Windows Client Installation Settings – Management Agent** page, click **Next**.

5 Perform the procedure to configure the Management Agent installation settings in Configuring the Management Agent installation settings.

6 (Optional) If you chose to enable Drive Encryption, on the **Windows Client Installation Settings – Drive Encryption** page, click **Next**. Then, perform the procedure to configure the Drive Encryption installation settings in Configuring the Drive Encryption installation settings.

Alternatively, if you chose to enable Symantec Endpoint Encryption for BitLocker instead of Drive Encryption, on the **Windows Client Installation Settings – BitLocker** page, click **Next**. Then, perform the procedure to configure the Symantec Endpoint Encryption for BitLocker installation settings in Configuring the Symantec Endpoint Encryption for BitLocker installation settings.

7 (Optional) If you chose to enable Removable Media Encryption, on the **Windows Client Installation Settings – Removable Media Encryption** page, click **Next**.

Then, perform the procedure to configure the Removable Media Encryption installation settings in Configuring the Removable Media Encryption installation settings.

8 Click **Finish**.

9 In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.

10 (Optional) Change the default package name to a name of your choice.

11 Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

**Configuring the Management Agent installation settings**

After you select the Symantec Endpoint Encryption features that you want to enable, the Windows Client installation settings wizard walks you through a series of panels, where you choose your Management Agent settings. This section contains the basic steps and information to configure the Management Agent installation settings in the Windows Client installation package. To learn more about any of the options, click the link at the end of each procedure.
To configure the Management Agent installation settings

Management Agent Installation Settings – Password Authentication page

1. On the **Windows Client Installation Settings – Management Agent** page, click **Next**.

2. On the **Management Agent Installation Settings – Password Authentication** page, do the following:
   - In the Simple Authentication section:
     - Select the **Enable simple authentication** option to let users authenticate at the preboot login screen using only a password.

   **Note**: If more than one user is registered on a client computer, simple authentication is not used; the detailed login screen appears, which requires a user name and domain as well.

   **Note**: If a user with simple authentication enabled forgets their password and invokes Drive Encryption Self-Recovery, they are prompted for their user name. This ensures that the self-recovery questions belong to that user.

   - In the Password Attempts section:
     - The **Limit password attempts** option is selected by default. This option configures a logon delay to protect against Dictionary attack tools. When the option is selected, it enables **After <x> incorrect attempts** and **pause for <x> minutes between further attempts**. You can change the number of incorrect attempts and the pause duration. After the maximum number of consecutive incorrect attempts is reached, there is a delay of one minute, by default. You can change the default value for Drive Encryption. The delay time is 20 seconds for Removable Media Encryption and you cannot change this default value.

   - In the Password Complexity section:
     - In the **Minimum password length** box, type the number of characters users' Removable Media Encryption file encryption passwords must contain. The default value is 8.

     - Provide values for the options available under the **Password must contain at least** box to bring more complexity to the user password. The options are **Non-alphanumeric characters**, **UPPERCASE letters**, **lowercase letters**, and **digits**.
- Add any non-alphanumeric characters that you want to allow in the password in the **Non-alphanumeric characters allowed in password** box. At any time, you can click **Restore Default** to remove the characters you have added manually.

  The Password Complexity settings are enforced only for Removable Media Encryption file encryption passwords.

- In the **Maximum Password Age** section:
  - If you do not want Removable Media Encryption file encryption passwords to expire, select **Password never expires**.
  - To set an expiration date on Removable Media Encryption file encryption passwords:
    - Select **Password expires every <x> days**. In the **Password expires every <x> days** box, type the number of days after which users' passwords expire.
    - In the **Warn users <x> before their passwords expire** box, type the number of days in advance users are prompted to change their expiring passwords.

  The Maximum Password Age settings are enforced only for Removable Media Encryption file encryption passwords.

- In the **Password History** section:
  - To allow users to use any previously used Removable Media Encryption file encryption passwords, leave the default selection of **Any previous password can be used**.
  - To define a password history restriction, select **The last <x> passwords cannot be reused**. In the **The last <x> passwords cannot be reused** box, type the number of different passwords that users must use before reverting to old passwords.

  The Password History settings are enforced only for Removable Media Encryption file encryption passwords.

3. Click **Next**.

   See “Configuring the Management Agent - Password Authentication policy options” on page 113.

### Management Agent Installation Settings – Communication page

1. On the **Management Agent Installation Settings – Communication** page, do the following:
   - In the **Send status updates every <x> minutes** box, specify how frequently the client should send status updates to Symantec Endpoint Encryption...
Management Server. The communication interval is set to 60 minutes by default.

- Verify the **Connection Name, Server, Name, Domain**, and type the password in the **Password** box under the **Communication information** section.

2. Click **Next** and then do one of the following:

- Configure the Drive Encryption installation settings.
  See “Configuring the Drive Encryption installation settings” on page 76.

- On the **Windows Client Installation Settings – BitLocker** page, click **Next**.

- Configure the Removable Media Encryption installation settings.
  See “Configuring the Removable Media Encryption installation settings” on page 86.

Alternatively, if you chose to enable only Symantec Endpoint Encryption for BitLocker, on the **Windows Client Installation Settings – BitLocker** page, click **Finish**, and then do the following:

- In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.

- (Optional) Change the default package name to a name of your choice.

---

**Note:** If you use a custom folder location, make sure that you install the Windows Password Reset Utility at the same location as Drive Encryption is installed.

---

- Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

  See “Configuring the Management Agent - Communication policy options” on page 115.

---

### Configuring the Drive Encryption installation settings

The Windows Client installation settings wizard walks you through a series of panels, where you choose your installation settings for the features that you chose to enable. This section contains the basic steps and information to configure the Drive Encryption installation settings in the Symantec Endpoint Encryption Client installation package. To learn more about any of the options, click the link at the end of each procedure.
Note: By default, the Symantec Endpoint Encryption Client installation package also installs the Symantec Endpoint Encryption Client Administrator Console and the Drive Encryption Administrator Command Line. No additional configuration is required to enable these features.

To configure the Drive Encryption installation settings

Drive Encryption Installation Settings – Client Administrators page


2. On the Drive Encryption Installation Settings – Client Administrators page, do one of the following:
   - Click Add to add a client administrator. Type the client administrator details in the Account Name, Password, and Confirm Password boxes. Check the administrative privileges that you want to assign to the client administrator. By default, the Default admin is checked that includes all of the available administrative privileges. To provide limited administrative privileges, uncheck Default admin and check one or more privileges that you want to assign from Admin Privileges. Click OK to save the newly added client administrator.
     You need to add a minimum of one client administrator to proceed to the next page of the Windows Client installation settings wizard.
   - Select an existing client administrator, and click Edit to edit an existing client administrator.
   - Select an existing client administrator, and click Delete to delete an existing client administrator. You must have at least one client administrator in the list to proceed to the next page.
   - The Action List makes available the options to Load client administrators from installation, Import client administrators from csv, and Export client administrators to csv. Click the link at the end of this procedure to see the Client Administrators policy options details for how to use these actions.

3. Click Next.

See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.

See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.
Drive Encryption Installation Settings – Registered Users page

1. On the Drive Encryption Installation Settings - Registered Users page, under Authentication Method, select an option from the Require registered users to authenticate with box to configure authentication method for Drive Encryption users.
   - (Default) To have users authenticate with a password, click **a password**.
   - To have users authenticate with a token, click **a token**.
   - To have users authenticate using either a password or a token, click **password or token**.

2. Under **User Registration**, select a user registration option to configure the user registration method for Drive Encryption users.
   - (Default) To allow users to authenticate and register using a Windows user name and a Windows password or token, click **Using Windows user authentication credentials**.
     
     **Note:** The single sign-on policy is applicable only to this type of users.

     - To allow users to authenticate and register using a Windows user name and a Drive Encryption password, click **Using Windows user name, non-Windows password**.
       
       **Note:** This option is not available if you have selected either **a token**, or **password or token**, from the Require registered users to authenticate with list box.

     - To allow users to authenticate and register using a Drive Encryption user name and a Drive Encryption password, click **Using non-Windows username, non-Windows password**.
       
       **Note:** This option is not available if you have selected either **a token**, or **password or token**, from the Require registered users to authenticate with list box.

3. Click **Next**.

   See “Configuring the Drive Encryption - Registered Users policy options” on page 122.
Drive Encryption Installation Settings – Single Sign-On page

1. On the **Drive Encryption Installation Settings - Single Sign-On** page, the **Enable Single Sign-On** option is checked by default. The selection of this option enables you to allow users to authenticate at preboot and directly access the client computer without authenticating at the Windows logon screen.

2. Click **Next**.
   
   See “Configuring the Drive Encryption - Single Sign-On policy options” on page 125.

Drive Encryption Installation Settings – Self-Recovery page

1. On the **Drive Encryption Installation Settings - Self-Recovery** page, the **Enable Self-Recovery** option is checked by default. The selection of this option enables you to provide values for the **Minimum answer length**, **Predefined questions**, and **Number of user-defined questions required** boxes.

2. Click **Next**.
   
   See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.

If you update this policy and your users no longer comply, the user is prompted to reconfigure their self-recovery question and answers. The prompt follows the following conditions:

- If the user has configured two questions and the policy is changed so that two questions come from the server, then the user is prompted to reconfigure their Drive Encryption self-recovery questions.

- If the user has configured two questions, and the policy is changed so that three questions are necessary, then the user is prompted to reconfigure their Drive Encryption self-recovery questions.

- If the user has configured three questions and now the policy has changed so that two questions are necessary, then the user is not prompted.

Drive Encryption Installation Settings – Startup page

1. In the **Preboot Splash Screen** section of the **Drive Encryption Installation Settings - Startup** page, do the following:

   - Click **A custom image** or **The SEE logo** to select the image that a user should see in the Drive Encryption startup screen. Alternatively, click **None** if you do not want a startup screen to precede the preboot authentication screen.
■ (Optional) If you selected A custom image, click Browse to select a custom image that is in the .xpm file format.

■ In the Text Color menu, click Black (default) or White to set the color of the legal notice text that appears on the startup screen. You can skip this step if you do not want to display a startup screen or a legal notice.

■ Enter the Legal Notice text that you want to display on the startup screen. By default, the Legal notice box contains a standard notice from Symantec.

■ Type the startup logon message in the Logon Message box that you want to display to registered users as they authenticate to Drive Encryption. The maximum number of characters displayed in the login screen is 80. In the Japanese version, the maximum is 40 because the double-byte characters occupy double the width of Latin characters.

Note: The maximum number of characters displayed in the preboot startup screen is 1024. There is also a limit of 19 lines of text; therefore, not all 1024 characters may be displayed as some longer words can cause lines to wrap early.

In the Chinese, Japanese, and Korean versions, the maximum number of characters displayed in the preboot splash screen is 512, instead of 1024. This is due to the double-byte characters occupying double the width of Latin characters when displayed.

2 In the Preboot Login Screen section, do the following:

■ Click A custom image or The SEE logo to select the image that a user should see in the Drive Encryption login screen. Alternatively, click None if you do not want a startup screen to precede the preboot authentication screen.

■ (Optional) If you selected A custom image, click Browse to select a custom image that is in the .xpm file format.

■ In the Text Color menu, click Black (default) or White to set the color of the logon message text that appears on the login screen.
In the **Logon Customization** section, type the logon message that you want to display at startup in the **Logon Message** box.

---

**Note:** The maximum number of characters displayed in the login screen is 80. In the Chinese, Japanese, and Korean versions, the maximum number of characters displayed in the login splash screen is 40, instead of 80. This is due to the double-byte characters occupying double the width of Latin characters when displayed.

---

4 Click **Next**.

   See “Configuring the Drive Encryption - Startup policy options” on page 126.

**Drive Encryption Installation Settings – Logon History page**

1 On the **Drive Encryption Installation Settings - Logon History** page, do the following:

   ■ Check or uncheck **User name**.

   ■ After you check this option, **Domain** disables, and prefills the Symantec Endpoint Encryption logon screen with the name and domain of the most recently logged on user.

2 Click **Next**.

   See “Configuring the Drive Encryption - Logon History policy options” on page 130.

**Drive Encryption Installation Settings – Encryption page**

1 On the **Drive Encryption Installation Settings - Encryption** page, do the following:

   ■ Click **128-bit** or **256-bit** to specify the AES encryption strength in the **AES encryption strength** box. **256-bit** is selected by default.

   ■ Select **Encrypt boot disk only** or **Encrypt all disks** to specify which disks you want to encrypt.

   ■ Check or uncheck **Include unused disk space when encrypting disks and partitions**. This check box is selected by default. After the selection of this option, Drive Encryption includes the encryption of the unused disk space when you encrypt the disks and partitions.

---

**Note:** Client administrators can use the Administrator Command Line to issue an `encrypt` command with a `--skip-unused-space` option, independent of this policy setting.
Check or uncheck Double-write sectors during encryption or decryption
(May significantly increase encryption and decryption time). After you
check this option, every data sector is double-written during fixed disk
encryption or decryption and may significantly increase encryption and
decryption time.

2 Click Next.

See “Configuring the Drive Encryption - Encryption policy options”
on page 130.

Drive Encryption Installation Settings – Client Monitor page

1 On the Drive Encryption Installation Settings - Client Monitor page, do one
of the following:

- The Do not enforce a minimum contact period with the SEE Management
  Server option is selected by default. After the selection of this option, you
cannot enforce a regular network contact.

- Click Lock computer after <x> days without contact to force a computer
  lockout after a specified number of days without network contact. If you
  select this option, you can specify the number of days a computer may
  remain without network contact, from 1–365. Type the number of days
  in advance, from 0–364 that users are warned to connect to the network
  and avoid a lockout in the Warn users <x> days before locking computer
  box.

2 Click Next.

See “Configuring the Drive Encryption - Client Monitor policy options”
on page 131.

Drive Encryption Installation Settings – Help Desk Recovery page

1 On the Drive Encryption Installation Settings - Help Desk Recovery page, do the following:

- The Enable Help Desk Recovery option is selected by default. The selection
  of this option enables you to make this pre-Windows authentication
  assistance method available to Drive Encryption users.

- Check or uncheck Help Desk Recovery Communication Unlock. After
  you check this option, it enables the users who have been locked out of
  their computers for a failure to communicate to regain access using the
  Help Desk Recovery Program.

2 Click Next.

See “Configuring the Drive Encryption - Help Desk Recovery policy options”
on page 132.
Drive Encryption Installation Settings – Self-Encrypting Drives page

1  On the **Drive Encryption Installation Settings - Self-Encrypting Drives** page, the **Use hardware encryption for compatible Opal-compliant drives** option is checked by default. The selection of this option allows hardware encryption on Opal v2 compliant drives using an Opal drive's built-in encryption capability.

For a detailed description of qualifying conditions that Opal v2 compliant drives must meet, see: http://www.symantec.com/docs/TECH226779.

**Note:** Drive Encryption software uses registry entries to identify which drives are whitelisted. When Symantec releases a new version of Endpoint Encryption, Symantec updates the whitelist and populates the registry entries as part of the release. If Symantec tests and approves Opal drives between releases, Symantec updates the whitelist but you must populate the new registry entries. You only need to do this if you are interested in using one or more of those drives. To see the process for creating registry entries that identify an Opal drive as whitelisted, see: http://www.symantec.com/docs/TECH235480.

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

See “Configuring the Removable Media Encryption installation settings” on page 86.

Alternatively, if you chose not to enable Removable Media Encryption, click **Finish**, and then do the following:

- In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.

- (Optional) Change the default package name to a name of your choice.

- Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

See “Configuring the Drive Encryption - Self-Encrypting Drives policy options” on page 132.
Configuring the Symantec Endpoint Encryption for BitLocker installation settings

The Windows Client installation settings wizard walks you through a series of panels, where you choose your installation settings for the features that you chose to enable. This section contains the basic steps and information to configure the Symantec Endpoint Encryption for BitLocker installation settings in the Symantec Endpoint Encryption Client installation package. To learn more about any of the options, click the link at the end of each procedure.

To configure the Symantec Endpoint Encryption for BitLocker installation settings

BitLocker Installation Settings – Encryption and Authentication page

1. On the Windows Client Installation Settings - BitLocker page, click Next.

2. On the BitLocker Installation Settings - Encryption and Authentication page, select an encryption or a decryption policy option.

3. For the encryption policy option, do the following to select the encryption and the authentication policies:

   - To encrypt all volumes on a client computer, select Encrypt all volumes. This option is checked by default.

   - In the Encryption Method section, you must select an encryption strength; you may select an encryption mode. For all Windows systems, select 128-bit or 256-bit in the AES encryption strength box to specify the AES encryption strength. For systems running Windows 10 version 1511 and later, optionally also select Prefer the XTS-AES encryption mode, if available. The AES encryption strength that you selected is applied.

   **Note:** If you are installing the BitLocker client on a system with Windows 10 version 1511 earlier installed with the Prefer the XTS-AES encryption mode, if available option selected, then the volumes are encrypted using the AES encryption mode only.

   - In the Authentication Method section, select an option to specify how users gain access to the client computer. Do one of the following:

     - To have users authenticate with TPM, click Trusted Platform Module (TPM). User intervention or credentials are not required to gain access to the client computer.

     - To have users authenticate with TPM and a PIN, click TPM and PIN. This option is selected by default. The PIN length must be 4 - 20 digits.
■ To use the password authentication method for the client computers that do not have TPM chip, or do not have TPM in a ready-to-use state, click **Fall back to password if TPM is unavailable**. This option is selected by default. The password length must be 8 - 99 characters. This policy option is supported on computers having operating system Windows 8 or later installed.

4 For the decryption policy option, select **Decrypt all volumes** to decrypt all the volumes on a client computer. Symantec Endpoint Encryption for BitLocker first decrypts all of the data volumes and then decrypts the boot volume.

5 Click **Next**.

See “Configuring the BitLocker Client - Encryption and Authentication policy options” on page 150.

**BitLocker Installation Settings - Client Monitor page**

1 On the **BitLocker Installation Settings - Client Monitor** page, choose one of the two options that you want to apply on a computer with Symantec Endpoint Encryption for BitLocker installed:

■ The **Do not enforce a minimum contact period with the SEE Management Server** option is selected by default. After the selection of this option, you cannot enforce a regular network contact.

■ Click **Lock computer after <x> days without contact** to force a computer lockout after a specified number of days without network contact. If you select this option, you can specify the number of days a computer may remain without network contact, from 1 - 365. Type the number of days in advance, from 0 - 364 that users are warned to connect to the network and avoid a lockout in the **Warn users <x> days before locking computer** box.

2 If you chose to enable Removable Media Encryption, click **Next** to configure the Removable Media Encryption installation settings. See “Configuring the Removable Media Encryption installation settings” on page 86.

Alternatively, if you chose not to enable Removable Media Encryption, click **Finish**, and then do the following:

■ In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.

■ (Optional) Change the default package name to a name of your choice.

■ Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.
Configuring the Removable Media Encryption installation settings

The Windows Client installation settings wizard walks you through a series of panels, where you choose your installation settings for the features that you chose to enable. This section contains the basic steps and information to configure the Removable Media Encryption installation settings in the Symantec Endpoint Encryption Client installation package. To learn more about any of the options, click the link at the end of each procedure.

About the Symantec Removable Media Encryption Burner Application

When Removable Media Encryption is installed on a client computer, the Symantec Removable Media Encryption Burner Application is also installed. The application requires the enablement of the Access and Encryption policy option 'Allow read and write access to files on removable media.'

The Symantec Removable Media Encryption Burner Application lets users encrypt and then burn files and folders onto CDs, DVDs, and Blu-ray Discs. From the client computer, a user can access the application in two ways:

- From the Windows Start menu, select Symantec Removable Media Burner Application. When the application launches, the user can access the online Help for instruction on using the interface.

- From the command line, run the Removable Media Encryption Burner Application command line. For more information, see the Symantec Endpoint Encryption 11.1.2 Removable Media Encryption Burner Application Command line Guide.

To configure the Removable Media Encryption installation settings

Removable Media Encryption Installation Settings - Access and Encryption page


2. On the Removable Media Encryption Installation Settings - Access and Encryption page, do the following:

   - In the Access section, do one of the following:

     - Click Do not allow access to files on removable media to deny read and write access to the files and folders that are stored on removable media, even if a user is registered to Symantec Endpoint Encryption.
Click **Allow read-only access to files on removable media** to allow the users to read the files that are stored on removable media. If the files are encrypted, users must provide the credentials that are used to encrypt the file to read its contents. In such a case, the users cannot write files to removable media.

Click **Allow read and write access to files on removable media** option to allow the users to read and write files to removable media. If the files are encrypted, users must provide the credentials that are used to encrypt the file to read its contents. This option is selected by default. When you select this option, the options for **Encryption Format**, **Automatic Encryption**, and **On-Demand Encryption** are available.

In the **Encryption Format** section, do one of the following:

- Click **SEE RME** to encrypt files to removable media using the Symantec Endpoint Encryption Removable Media Encryption 11.x format. This option is selected by default.
- Click **SEE RS** to encrypt files to removable media using the Symantec Endpoint Encryption Removable Storage 8.2.1 format. Select this option if your users move files between the computers that are running 11.x and 8.2.1 software. This encryption format is backward-compatible and computers running either version of the software can read these files.

In the **Automatic Encryption** section, do one of the following:

- Click **Do not encrypt** not to encrypt files on removable media.
- Click **Encrypt files as per Symantec Data Loss Prevention** to use the detection and the response capabilities of Symantec Data Loss Prevention to dictate the encryption of files.
- Click **Encrypt new files** to automatically encrypt all files newly added to removable media. This option is selected by default.

**Note:** To exclude multimedia files or certain file types from automatic encryption, you can select more options on the **Device and File Type Exclusions** page.

Click **Allow users to choose** if you want to let the users choose whether or not to automatically encrypt new files. Under the **Allow users to choose** option, select the default behavior that you want to happen if your users do not make a choice. Choose either **Default to encrypt new files**, or **Default to do not encrypt**.
In the **On-Demand Encryption** section, you can:

- **Check Users can right-click to encrypt existing files on removable media** to provide the users with the ability to encrypt files on removable media using a right-click menu. This option is selected by default.

- **Check Users can right-click to decrypt existing files on removable media** to provide the users with the ability to decrypt files on removable media using a right-click menu.

  If **Encrypt files as per Symantec Data Loss Prevention** is selected, Symantec recommends unchecking both options.

3. **Click Next.**


**Removable Media Encryption Installation Settings - Device and File Type Exclusions page**

1. **On the Removable Media Encryption Installation Settings - Device and File Type Exclusions page**, do the following:

   - **In the Exemption for Multimedia Files section**, check or uncheck **Exclude multimedia files from automatic encryption**. Even if you select the **Encrypt new files** option on the **Access and Encryption** page, you can exempt certain types of multimedia files from automatic encryption by checking **Exclude multimedia files from automatic encryption**. Then leave selected one or more of the following check boxes according to the type of multimedia file formats you want to exclude from encryption:

     - **Audio**
       
       See “Audio file types excluded” on page 289.

     - **Video**
       
       See “Video file types excluded” on page 292.

     - **Image**
       
       See “Image file types excluded” on page 296.

   - **In the File Types Exclusion section,**

     - **Check or uncheck Exclude file types extensions from automatic encryption (comma separated)**. Check this option, and type the file type extensions, such as .jpeg, .exe, and so on that are excluded from automatic encryption.
In the **Device Exclusions** section, check or uncheck **Exclude these removable media encryption devices from encryption**. Do one of the following to exempt removable media encryption devices from encryption:

- To exempt a specific device from a vendor, enter the vendor ID, product ID, and an optional description in the fields provided.
- To exempt all the devices from a vendor, type the vendor ID in the **Vendor ID** box. Also type the wildcard character * in the **Product ID** box and an optional description in the **Description (Optional)** box.

2 Click **Next**.

See “Configuring the Removable Media Encryption - Device and File Type Exclusions policy options” on page 139.

**Removable Media Encryption Installation Settings - Encryption Method page**

1 On the **Removable Media Encryption Installation Settings - Encryption Method** page, do one of the following:

- The **A password** option is selected by default. The selection of this option enables the users to restrict the encryption method to a password.
- Click **A certificate** so that users can restrict the encryption method to one certificate.
- Click **A password and/or certificate** to let each user choose the encryption method of password, certificate, or both.

2 Click **Next**.

See “Configuring the Removable Media Encryption - Encryption Method policy options” on page 140.

**Removable Media Encryption Installation Settings - Default Passwords page**

1 On the **Removable Media Encryption Installation Settings - Default Passwords** page, do the following:

- In the **Default Password** section, do one of the following:
  - To allow users to set a default password, click **Allow users to set a default password**. This option is chosen by default.
  - To apply password aging to default passwords, check **Apply password aging to Removable Media Encryption default passwords**. This option ensures that users set default passwords that conform to the restrictions that you define. These restrictions are defined in the **Maximum Password Age** and **Password History** sections of the Management Agent Password Authentication policy. These settings define expiration dates and restrict password reuse.
Note: If you let users set a default password, you can also let them set session passwords. You cannot allow both default passwords and device session passwords to be set.

- To prevent users from setting a default password, click **Do not allow users to set a default password**.

- If the **Session Passwords** section is available, do one of the following:
  - To allow users to set session passwords, click **Allow users to set session passwords**; otherwise, click **Do not allow users to set session passwords**.
  
  If you let users set session passwords, choose the password expiration method:
  - To permanently expire (delete) session passwords at the end of each Windows session, click **Delete session passwords at the end of every Windows session**. Users must recreate the passwords.
  - To temporarily expire (deactivate) session passwords at the end of each Windows session, click **Deactivate session passwords at the end of every Windows session, but allow them to persist across every Windows session**. Passwords remain on the user's computer, but the user must toggle them on.
  - To apply password aging to session passwords, click **Apply password aging to session passwords**. This option ensures that users set session passwords that conform to the restrictions that you define. These restrictions are defined in the **Maximum Password Age** and **Password History** sections of the Management Agent Password Authentication policy. These settings define expiration dates and restrict password reuse.
  - To prevent session passwords from expiring, click **Do not delete or deactivate session passwords**. This option is chosen by default.

- If the **Device Session Password** section is available, do one of the following:
  - To allow users to set device session passwords, click **Allow users to set a device session password for each removable media encryption device**. Device session passwords are useful in a kiosk environment.

Note: If you enable device session passwords, you cannot use recovery certificates. Even if you enable certificates on the **Recovery Certificate** page, Removable Media Encryption ignores them.
If you do not want users to set device session passwords, click **Do not allow users to set a device session default password for each removable device**. This option is chosen by default.

2 Click **Next**.

See “Configuring the Removable Media Encryption - Default Passwords policy options” on page 140.


See “Configuring the Management Agent installation settings” on page 73.

**Removable Media Encryption Installation Settings - Recovery Certificate page**

**Note:** Use the Recovery Certificate policy to include the copy of the Recovery Certificate that does not have the private key in the Removable Media Encryption package. Upon receipt, clients begin to encrypt files using this Recovery Certificate in addition to the user’s credentials. The Recovery Certificate policy only applies to computers on which write access and encryption are enabled for removable media devices.

1 On the **Removable Media Encryption Installation Settings - Recovery Certificate** page, do one of the following:

- Click **Do not encrypt files with a recovery certificate** not to include a copy of the Recovery Certificate in the client installation package. This option is selected by default.

- Click **Encrypt files with a recovery certificate** if you want to use a Recovery Certificate.

**Note:** If you enable device session passwords on the **Default Passwords** page, Removable Media Encryption ignores recovery certificates.

- You are prompted for the location of the PKCS#7 format certificate file (.p7b), choose a certificate file.

- Click **OK**.
On the **Recovery Certificate** page, the issuer and serial number of the certificate appears. Click **Change Certificate** to select a different certificate file.

2 **Click Next.**


See “Configuring the Removable Media Encryption - Default Passwords policy options” on page 140.

**Removable Media Encryption Installation Settings - Portability page**

1 On the **Removable Media Encryption Installation Settings - Portability** page, do the following:

   ■ In the **Access Utility** section:

     ■ Check or uncheck **Copy the Removable Media Access Utility for Windows to removable media**. After you check this option, it enables you to write Removable Media Access Utility that runs on Windows computers to removable media automatically.

     ■ Check or uncheck **Copy the Removable Media Access Utility for Mac OS X to removable media**. After you check this option, it enables you to write Removable Media Access Utility that runs on Mac OS X computers to removable media automatically.

   ■ In the **Self-Decrypting Archive** section:

     ■ Check or uncheck **Allow users to save files as password encrypted self-decrypting archive**. After you check this option, it enables you to permit users to create self-decrypting archives.

2 **Click Next.**

See “Configuring the Removable Media Encryption - Portability policy options” on page 144.

**Removable Media Encryption Installation Settings - Expired Certificates page**

1 On the **Removable Media Encryption Installation Settings - Expired Certificates** page, do one of the following:

   ■ Check **Users can use expired certificates to encrypt files** so that the user can encrypt the file using an expired certificate.

   ■ If you uncheck this option, the user cannot use an expired certificate for file encryption.

2 **Click Finish.**
3 In the **Save MSI Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption Client installation package.

4 (Optional) Change the default package name to a name of your choice.

5 Click **Save** to create the Symantec Endpoint Encryption Client installation package at the selected location.

---

**About enabling features in the Symantec Endpoint Encryption Client installation package**

When you create a Symantec Endpoint Encryption Client installation package, you enable features depending upon your organization’s security requirements. Use the Windows Client Installation Settings wizard to specify the features that you want to enable in Symantec Endpoint Encryption Client. The Symantec Endpoint Encryption Client installation package contains the policy settings for all of the features that you enable. This topic provides information about enabling features in the Symantec Endpoint Encryption Client installation package.

On the **Windows Client Installation Settings – Features** page of the Windows Client Installation Settings wizard, you can choose to enable the following features:

- For disk encryption:
  - Drive Encryption, or
  - Symantec Endpoint Encryption for BitLocker
- Removable Media Encryption

You cannot install both Drive Encryption and Symantec Endpoint Encryption for BitLocker on the same client computer. If you already have Drive Encryption installed, you cannot enable Symantec Endpoint Encryption for BitLocker. Similarly, if you already have Symantec Endpoint Encryption for BitLocker installed, you cannot enable Drive Encryption. However, you can enable Removable Media Encryption with either feature.

**Enabling additional features on Microsoft Windows clients**

You can create and deploy a new Symantec Endpoint Encryption Client installation package to modify the number of features that are installed on version 11.1.2 client computers. First ensure that the disk is already fully encrypted or decrypted. If disk encryption or decryption is in progress, wait until the operation is complete before you deploy the installation package.

For information about deploying the Symantec Endpoint Encryption Client installation package to install additional features on client computers, see Deployment client installers using the command line.
Note: You cannot use the Windows Client Installation Settings wizard to remove features from client computers. You must uninstall the unwanted features individually. See “About uninstalling the Symantec Endpoint Encryption client” on page 277.

See “Creating a Symantec Endpoint Encryption Client installation package” on page 72.

### Table 4-1 Modifying features in the Symantec Endpoint Encryption Client installation package

<table>
<thead>
<tr>
<th>Features that are already installed</th>
<th>Features that you want to add</th>
<th>Features that you must enable in the client installation package</th>
</tr>
</thead>
</table>
| Drive Encryption                   | Removable Media Encryption  | ■ Drive Encryption  
■ Removable Media Encryption  
OR  
Removable Media Encryption only |
| Removable Media Encryption         | Drive Encryption            | ■ Drive Encryption  
■ Removable Media Encryption  
OR  
Drive Encryption only |
| Removable Media Encryption         | Symantec Endpoint Encryption for BitLocker | ■ Symantec Endpoint Encryption for BitLocker  
■ Removable Media Encryption  
OR  
Symantec Endpoint Encryption for BitLocker only |

- ■ Symantec Endpoint Encryption for BitLocker  
■ Removable Media Encryption  

- ■ Drive Encryption  
■ Removable Media Encryption  

This is not a valid feature combination.
## Enabling features during upgrades

The following tables provide feature selection information for upgrades, depending upon the product and version that is currently installed.

### Table 4-2

**Enabling features when upgrading from Symantec Endpoint Encryption 11.0.x or later**

<table>
<thead>
<tr>
<th>Features that are already installed</th>
<th>Additional 11.1.2 features that you want to install during the upgrade</th>
<th>Features that you must enable in the client installation package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive Encryption</td>
<td>None</td>
<td>Drive Encryption</td>
</tr>
<tr>
<td>Removable Media Encryption</td>
<td>None</td>
<td>Removable Media Encryption</td>
</tr>
<tr>
<td>Drive Encryption</td>
<td>Removable Media Encryption</td>
<td>▪ Drive Encryption ▪ Removable Media Encryption</td>
</tr>
<tr>
<td>Removable Media Encryption</td>
<td>Drive Encryption</td>
<td>▪ Drive Encryption ▪ Removable Media Encryption</td>
</tr>
<tr>
<td>Drive Encryption</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>This is not a valid feature combination.</td>
</tr>
<tr>
<td>Removable Media Encryption</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>▪ Symantec Endpoint Encryption for BitLocker ▪ Removable Media Encryption</td>
</tr>
<tr>
<td>▪ Drive Encryption ▪ Removable Media Encryption</td>
<td>None</td>
<td>▪ Drive Encryption ▪ Removable Media Encryption</td>
</tr>
<tr>
<td>▪ Drive Encryption ▪ Removable Media Encryption</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>This is not a valid feature combination.</td>
</tr>
</tbody>
</table>
### Table 4-3  Enabling features when upgrading from Symantec Endpoint Encryption 8.2.1

<table>
<thead>
<tr>
<th>Features that are already installed</th>
<th>Additional 11.1.2 features that you want to install during the upgrade</th>
<th>Features that you must enable in the client installation package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Encryption Full Disk</td>
<td>None</td>
<td>Drive Encryption</td>
</tr>
<tr>
<td>Symantec Endpoint Encryption Removable Storage</td>
<td>None</td>
<td>Removable Media Encryption</td>
</tr>
<tr>
<td>Symantec Endpoint Encryption Full Disk</td>
<td>Removable Media Encryption</td>
<td>■ Drive Encryption  ■ Removable Media Encryption</td>
</tr>
<tr>
<td>Symantec Endpoint Encryption Removable Storage</td>
<td>Drive Encryption</td>
<td>■ Drive Encryption  ■ Removable Media Encryption</td>
</tr>
<tr>
<td>Symantec Endpoint Encryption Full Disk</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>This is not a valid feature combination.</td>
</tr>
<tr>
<td>Symantec Endpoint Encryption Removable Storage</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>■ Symantec Endpoint Encryption for BitLocker  ■ Removable Media Encryption</td>
</tr>
<tr>
<td>■ Symantec Endpoint Encryption Full Disk  ■ Symantec Endpoint Encryption Removable Storage</td>
<td>None</td>
<td>■ Drive Encryption  ■ Removable Media Encryption</td>
</tr>
<tr>
<td>■ Symantec Endpoint Encryption Full Disk  ■ Symantec Endpoint Encryption Removable Storage</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>This is not a valid upgrade.</td>
</tr>
</tbody>
</table>

### Table 4-4  Enabling features when upgrading from Symantec Encryption Desktop 10.3.2 MP4 for Windows, or later

<table>
<thead>
<tr>
<th>Features that are already installed</th>
<th>Additional 11.1.2 features that you want to install during the upgrade</th>
<th>Features that you must enable in the client installation package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Encryption Desktop</td>
<td>None</td>
<td>Drive Encryption</td>
</tr>
</tbody>
</table>
Table 4-4  Enabling features when upgrading from Symantec Encryption Desktop 10.3.2 MP4 for Windows, or later (continued)

<table>
<thead>
<tr>
<th>Features that are already installed</th>
<th>Additional 11.1.2 features that you want to install during the upgrade</th>
<th>Features that you must enable in the client installation package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Encryption Desktop</td>
<td>Removable Media Encryption</td>
<td>■ Drive Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Removable Media Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enable only Removable Media Encryption, if you do not want to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>upgrade to Drive Encryption.</td>
</tr>
<tr>
<td>Symantec Encryption Desktop (with</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>This is not a valid upgrade.</td>
</tr>
<tr>
<td>the Symantec Drive Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>feature enabled)</td>
<td>■ Symantec Endpoint Encryption for BitLocker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ Removable Media Encryption</td>
<td></td>
</tr>
<tr>
<td>Symantec Encryption Desktop (with</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td>This is not a valid upgrade.</td>
</tr>
<tr>
<td>the Symantec Drive Encryption</td>
<td>■ Symantec Endpoint Encryption for BitLocker</td>
<td></td>
</tr>
<tr>
<td>feature disabled)</td>
<td>■ Removable Media Encryption</td>
<td></td>
</tr>
<tr>
<td>Symantec Encryption Desktop (with</td>
<td>Symantec Endpoint Encryption for BitLocker</td>
<td></td>
</tr>
<tr>
<td>the Symantec Drive Encryption</td>
<td>■ Symantec Endpoint Encryption for BitLocker</td>
<td></td>
</tr>
<tr>
<td>feature disabled)</td>
<td>■ Removable Media Encryption</td>
<td></td>
</tr>
</tbody>
</table>

Creating a Symantec Endpoint Encryption for FileVault installation package

The Mac FileVault Client installation wizard walks you through a series of panels, where you choose your policy settings. You must perform the following steps to successfully create a Symantec Endpoint Encryption for FileVault installation package from the Management Console.

To create a Symantec Endpoint Encryption for FileVault installation package

1. In the left pane, click **Symantec Endpoint Encryption Software Setup > Mac FileVault Client**.
2. On the **Create Mac OS X Installer - Introduction** page, click **Next**.
3 On the **Create Mac OS X Installer – Institutional Recovery Key** page, do the following:

- (Default) Select the **Use an Institutional Recovery Key** check box. The selection of this option enables you to include an Institutional Recovery Key certificate in the install-time policy.
- Click **Change Key** to locate the path of the Institutional Recovery Key certificate, and select it.
- After you select the Institutional Recovery Key certificate, the name of the provider and the serial number of the Institutional Recovery Key appear in the **Issued By** and **Serial** boxes on the **Create Mac OS X Installer – Institutional Recovery Key** panel. To select a different Institutional Recovery Key certificate file, click **Change Key**.

4 Click **Next**.

5 On the **Create Mac OS X Installer - Communication** page, do the following:

- In the **Send status updates every <x> minutes** box, specify how frequently the Symantec Endpoint Encryption for FileVault client should send status updates to Symantec Endpoint Encryption Management Server. The communication interval is set to 60 minutes by default.
- Verify the **Connection Name, Server, Name, Domain**, and type the password in the **Password** box under the **Communication information** section.

6 Click **Finish**.

7 In the **Save Mac Package** dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption for FileVault installation package.

8 If required, change the default Symantec Endpoint Encryption for FileVault package name.

9 Click **Save** to create the Symantec Endpoint Encryption for FileVault installer with the administrative policies you have configured at your desired location.

See “Configuring the Mac FileVault Client - Introduction policy options” on page 147.

See “Configuring the Mac FileVault Client - Institutional Recovery Key policy options” on page 148.

See “Configuring the Mac FileVault Client - Communication policy options” on page 149.
Creating a Windows Password Reset Utility installation package

The Symantec Endpoint Encryption Windows Password Reset snap-in enables you to create a Windows Password Reset Utility installation package. When you install the Windows Password Reset Utility on a Drive Encryption client computer, the utility extends the functionality of the Drive Encryption Self-Recovery feature and the Help Desk Recovery feature to enable users to reset their Windows password by themselves. Use the Windows Password Reset Utility to reduce support calls to the local help desk when users forget their Windows password.

**Note:** To create a Windows Password Reset Utility installation package, you must have either the Server Administrator role or the Setup Administrator role. If the policy administrator enabled the Windows Password Reset using Drive Encryption Self-Recovery, existing registered users are automatically prompted to reconfigure their security questions and answers in Drive Encryption Self-Recovery wizard after the Windows Password Reset Utility is installed.

**To create a Windows Password Reset Utility MSI file**

1. In the left pane of the Management Console, click the **Symantec Endpoint Encryption Windows Password Reset** snap-in.
2. On the **Windows Password Reset - Management Password Authentication** page, in the **Management** Password field, type the management password.
3. Click **Next**.
4. On the **Windows Password Reset - Settings** page, check one or more of the following options:
   - **Drive Encryption Self-Recovery** - Enables users to reset their Windows password using the Drive Encryption Self-Recovery feature.
   - **Help Desk Recovery** - Enables users to reset their Windows password using the Help Desk Recovery feature.
5. Click **Finish** and save the MSI file at the desired location.

**Note:** If you use a custom folder location, make sure that you install the Windows Password Reset Utility at the same location as Drive Encryption is installed.
Creating Symantec Endpoint Encryption client installers

Creating a Windows Password Reset Utility installation package
Deploying new Symantec Endpoint Encryption clients

This chapter includes the following topics:

■ Deploying client packages using a third-party tool
■ Deploying new clients using Group Policy Objects
■ Installing the client software manually
■ Installing the Windows Password Reset Utility on a client computer
■ Deploying client installers using the command line

Deploying client packages using a third-party tool

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

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

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

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

Creating Symantec Endpoint Encryption Client installers for distribution

To create Symantec Endpoint Encryption client installers for distribution

- Create the MSI file for Symantec Endpoint Encryption Client. Choose the 32-bit or 64-bit version, as appropriate for the version of Microsoft Windows installed on your client computers.

For more information about creating the Symantec Endpoint Encryption Client installation package, see the *Creating Symantec Endpoint Encryption client installers* chapter available in the *Symantec Endpoint Encryption Management Server Online Help*.

See “Creating a Symantec Endpoint Encryption Client installation package” on page 72.

Creating an Active Directory distribution point

To create a distribution point on your Active Directory forest or domain

1. Save the created MSI file that you want to deploy using a GPO in a folder that is in a shared network location. For example, the location can be the domain controller's SYSVOL folder. The created folder is the distribution point on your Active Directory forest or domain.

2. Set the folder properties to enable users to have read and execute permissions. For example, you can avoid access permission issues during deployment if you set the security property of the shared folder to **Everyone**.

**Caution:** Carefully review your procedures on your network and follow the rights assignment policies of your organization. Reset the security property of the shared folder immediately when you finish deployment.
Creating GPOs to deploy the installer MSI
To create Group Policy Objects and deploy the client installer

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

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

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

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

10. In the **Deploy Software** dialog box, accept the default value of **Assigned** and click **OK** one or more times as prompted.
11. Close the **Group Policy Management Editor**.
Installing the client installer GPOs
After the deployment is complete, to begin the software installation, restart the client computers.

Installing the client software manually

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

Preparing to install the client software manually
Before installing the client software, you must do the following:

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

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

Installing Symantec Endpoint Encryption Client
To manually install Symantec Endpoint Encryption Client

1. Double-click the SEE Windows Client.msi file or the SEE Windows Client_x64.msi file.

2. When prompted to restart, click Yes to restart your system and complete the installation.
Installing Symantec Endpoint Encryption for FileVault

To manually install Symantec Endpoint Encryption for FileVault

1. Double-click the SEEInstaller-<version> installation package file, where <version> is the version number of the Symantec Endpoint Encryption for FileVault.

2. On the Welcome to the Symantec Endpoint Encryption Installer window, click Continue.

3. Read and agree to the Software license agreement and complete the installation.

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

Installing the Windows Password Reset Utility on a client computer

When you install the Windows Password Reset Utility on a Drive Encryption client computer, the utility extends the functionality of the Drive Encryption Self-Recovery feature to enable users to reset their Windows password by themselves. Use the Windows Password Reset Utility to reduce support calls to the local help desk when users forget their Windows password.

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

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

1. Navigate to the folder in which you saved the Windows Password Reset Utility client MSI file that you want to install.

2. Double-click the MSI file.

3. When prompted to restart, click Yes to restart your system and complete the installation.

See “Configuring the Drive Encryption - Windows Password Reset policy option” on page 133.
Deploying client installers using the command line

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

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

To run the Symantec Endpoint Encryption Client installer

1. Copy the installation .MSI file to the local hard disk of the computer on which you want to run the installer.
   - If the computer's operating system is 32-bit, copy the SEE Client.msi file.
   - If the computer's operating system is 64-bit, copy the SEE Client x64.msi file.

2. Depending on the version of Microsoft Windows, do one of the following:
   - **Windows 7** – Click **Start > All Programs > Accessories**. Right-click **Command Prompt** and select **Run as administrator**. If you are prompted, enter the credentials of a domain administrator account.
   - **Windows 8.x** – From the **Start** screen, access the **Apps** menu. In the **Windows System** section, right-click **Command Prompt** and select **Run as administrator**. If you are prompted, enter the credentials of a domain administrator account.
   - **Windows 10** – Click **Start > All apps**. In the **Windows System** section, right-click **Command Prompt** and select **Run as administrator**. If you are prompted, enter the credentials of a domain administrator account.

3. In the Command Prompt window, enter one of the following commands:
   - To perform a fresh installation:
     ```cmd
     MSIEXEC /i "[path]\msifile" /l*v "[logpath]\logfile"
     ```
   - To modify an existing setup by installing an additional feature:
     ```cmd
     MSIEXEC /i "[path]\msifile" REINSTALLMODE=vemus ADDLOCAL=ALL /l*v "[logpath]\logfile"
     ```
Where [path]\msifile represents the path and name of the MSI file, and [logpath]\logfile represents the path and name of the output log file.

4 When prompted, close the Command Prompt window and restart the computer.
Deploying new Symantec Endpoint Encryption clients

Deploying client installers using the command line
Configuring the Symantec Endpoint Encryption policy options

This chapter includes the following topics:

- About configuring the Symantec Endpoint Encryption policy options
- Accessing the Symantec Endpoint Encryption policy options
- Configuring the Management Agent policy options - process overview
- Configuring the Drive Encryption policy options - process overview
- Configuring the Removable Media Encryption policy options - process overview
- Configuring the Mac FileVault Client policy options - process overview
- Configuring the BitLocker Client policy options - process overview

About configuring the Symantec Endpoint Encryption policy options

Symantec Endpoint Encryption uses the policies that you configure and deploy to client computers, where the policies specify user and computer capabilities. For the Windows client computers, these policies are specific to Drive Encryption, Removable Media Encryption, and Symantec Endpoint Encryption for BitLocker, as well as to general system components and communication defined in the Management Agent settings. The policy options are grouped as follows:

- Management Agent
See “Configuring the Management Agent policy options - process overview” on page 112.

■ Drive Encryption
  See “Configuring the Drive Encryption policy options - process overview” on page 115.

■ Removable Media Encryption
  See “Configuring the Removable Media Encryption policy options - process overview” on page 134.

■ Symantec Endpoint Encryption for BitLocker
  See “Configuring the BitLocker Client policy options - process overview” on page 150.

For the Macintosh computers, you can configure the policy options for Symantec Endpoint Encryption for FileVault using Mac FileVault Client.

See “Configuring the Mac FileVault Client policy options - process overview” on page 146.

To initially define the policies:

■ Use the Management Console - Symantec Endpoint Encryption Software Setup menu to select each of the following installation wizards: Windows Client and Mac FileVault Client.

■ For instructions on how to navigate these wizards:
  See “Creating a Symantec Endpoint Encryption Client installation package” on page 72.
  See “Creating a Symantec Endpoint Encryption for FileVault installation package” on page 97.

After you define and install the policies, you can change them over time, as required. You have the following options available from the Management Console:

■ Use Active Directory (Group Policy Management snap-in)
  See “Managing GPOs - process overview” on page 154.

■ Use native policies (Symantec Endpoint Encryption Native Policy Manager)
  See “Managing native policies - process overview” on page 158.

■ Whether using GPO or native policies, refer to the configuration sections in this chapter for a specific policy, as appropriate.

---

**Note:** For Mac FileVault Client, you can define policy options to create the install-time policy. You cannot change the Mac FileVault Client install-time policy options using GPO or Native policies.
Accessing the Symantec Endpoint Encryption policy options

As a policy administrator, you may need to access policy options in the following cases:

- When you configure installation policies, resulting in the client installation package
- When you configure and deploy an Active Directory policy
- When you configure and deploy a native policy

**Note:** Some of the policies and options vary, depending on whether the policy is created as an installation setting or a policy update. For example, the Drive Encryption - Encryption policy options are available as an installation setting but not as an Active Directory policy or native policy.

**To access the Symantec Endpoint Encryption policy options**

1. From the Management Console, do one of the following:
   - To access installation policy options, in the left pane, click **Symantec Endpoint Encryption Software Setup**.
   - To access Active Directory policy options, in the left pane, click **Group Policy Manager**.
   - To access native policy options, in the left pane, click **Symantec Endpoint Encryption Native Policy Manager**.

2. Based on the functionality for which you want to configure the policy options, select one of the following:
   - **Windows Client**
   - **Mac FileVault Client**

3. To save the policy options, do one of the following:
   - To proceed to the next page in the install-time policy or native policy page, click **Next**.
   - To save the install-time policy settings and create the client installation package, click **Finish**.
   - To save the Active Directory policy settings, click **Save**.
   - To save the Native policy settings, click **Finish**.
Configuring the Management Agent policy options - process overview

You can configure the Management Agent policy options as described in the following table.

<table>
<thead>
<tr>
<th>Management Agent policy</th>
<th>Link to configure policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Authentication</td>
<td>To configure the Password Authentication policy option: Configuring the Management Agent - Password Authentication policy options</td>
</tr>
<tr>
<td>Communication</td>
<td>To configure the Communication policy option: Configuring the Management Agent - Communication policy options</td>
</tr>
</tbody>
</table>

See “Configuring the Management Agent installation settings” on page 73.
Configuring the Management Agent - Password Authentication policy options

To configure the Management Agent - Password Authentication policy options

1. Access the Management Agent policy options using an install-time, Active Directory, or native policy. On the Management Agent - Password Authentication page, take the actions that are described for each section.

2. In the Simple Authentication section, do the following:
   - Select the Enable simple authentication option to let users authenticate at the preboot login screen using only a password.

   **Note:** If more than one user is registered on a client computer, simple authentication is not used; the detailed login screen appears, which also requires a user name and domain.

   **Note:** If a user with simple authentication enabled forgets their password and invokes Drive Encryption Self-Recovery, they are prompted for their user name. This ensures that the self-recovery questions belong to that user.

3. In the Password Attempts section, do the following:
   - Select Limit password attempts to configure the number of password attempts allowed. This option is selected by default. If this option is selected, also do the following:
     - In the After <x> incorrect attempts box, type the number of incorrect password attempts that is allowed to occur before the delay is instituted.
     - For passwords that are used in Drive Encryption, in the pause for <x> minutes between further attempts box, type the length of the delay. After the maximum number of consecutive incorrect attempts is reached, there is a delay of one minute, by default. You can change the default value for Drive Encryption. The delay time is 20 seconds for Removable Media Encryption and you cannot change this value.

4. In the Password Complexity section, do the following:
   - In the Minimum password length box, type the number of characters a user's Symantec Endpoint Encryption password must contain.
In the **Non-alphanumeric characters allowed in password** box, type the set of non-alphanumeric characters that a user can have in their password. At any time, you can click **Restore Default** to remove the characters you have added manually and restore the original list.

In the **Password must contain at least** box, click the number for the following boxes to define the least number of those characters that users can have in their password:

- **non-alphanumeric characters**
- **UPPERCASE letters (A-Z)**
- **lowercase letters (a-z)**, and
- **digits (0-9)**

The **Password Complexity** settings are enforced only for Removable Media Encryption file encryption passwords.

5 In the **Maximum Password Age** section:

- If you do not want Removable Media Encryption file encryption passwords to expire, select **Password never expires**.

- To set an expiration date on passwords:
  - Select **Password expires every <x> days**. In the **Password expires every <x> days** box, type the number of days after which users' passwords expire.
  - In the **Warn users <x> days before their passwords expire** box, type the number of days in advance that the users are prompted to change their expiring passwords.

The **Maximum Password Age** settings are enforced only for Removable Media Encryption file encryption passwords.

6 In the **Password History** section:

- To allow users to reuse any previous Removable Media Encryption file encryption passwords, select **Any previous password can be used**.

- To define a password history restriction, select **The last <x> passwords cannot be reused**. In the **The last <x> passwords cannot be reused** box, type the number of different passwords that users must use before reverting to previously used passwords.

The **Password History** settings are enforced only for Removable Media Encryption file encryption passwords.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.
Configuring the Management Agent - Communication policy options

In the Management Agent - Communication policy, the full set of options is available only during installation. An Active Directory or native policy allows the update of the communication interval only.

To configure the Management Agent - Communication policy option

1. On the Management Agent - Communication page, in the Communication section for install-time, Active Directory, and native policy, do the following:
   - In the Send status updates every <x> minutes box, enter the interval, in minutes at which the Symantec Endpoint Encryption client reports any changes in its status data. The changes are reported to the selected Management Server. The default value is 60 minutes.

2. In the Communication Information section (installation policy only), do the following:
   - Connection Name displays the name of Symantec Endpoint Encryption Management Server.
   - Server displays the URL of the Web service running on the selected Management Server, including its NetBIOS name or FQDN and port number.
   - Name and Domain are prefilled with the name and domain of the IIS client account.
   - Type the password of this account in the Password box.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Drive Encryption policy options - process overview

You can configure the Drive Encryption policy options as described in the following table.
<table>
<thead>
<tr>
<th>Drive Encryption policy</th>
<th>Link to configure the policy options</th>
</tr>
</thead>
</table>
| Client Administrators             | To configure the Client Administrators policy options:  
|                                   | Configuring the Drive Encryption - Client Administrators policy options, for adding or editing     |
|                                   | Configuring the Drive Encryption - Client Administrators policy options, for deleting                |
| Registered Users                  | To configure the authentication method for registered users:  
|                                   | Configuring the Drive Encryption - Registered Users policy options                                 |
| Single Sign-On                    | To configure the Single Sign-On policy options:  
|                                   | Configuring the Drive Encryption - Single Sign-On policy options                                   |
| Self-Recovery                     | To configure the Self-Recovery policy options:  
|                                   | Configuring the Drive Encryption - Self-Recovery policy options                                    |
| Startup                           | To configure the Startup policy options:  
|                                   | Configuring the Drive Encryption - Startup policy options                                          |
| Logon History                     | To configure the Logon History policy options:  
|                                   | Configuring the Drive Encryption - Logon History policy options                                    |
| Encryption                        | To configure the Encryption policy options:  
|                                   | Configuring the Drive Encryption - Encryption policy options                                       |
| Client Monitor                    | To configure the Drive Encryption Client Monitor policy options:  
|                                   | Configuring the Drive Encryption - Client Monitor policy options                                    |
| Help Desk Recovery                | To configure the Help Desk Recovery policy options:  
|                                   | Configuring the Drive Encryption - Help Desk Recovery policy options                              |
| Self Encrypting Drives            | To configure the Self Encrypting Drives policy options:  
|                                   | Configuring the Drive Encryption - Self-Encrypting Drives policy options                           |
Table 6-2  Drive Encryption policy options (continued)

<table>
<thead>
<tr>
<th>Drive Encryption policy</th>
<th>Link to configure the policy options</th>
</tr>
</thead>
</table>
| Windows Password Reset  | To configure the Windows Password Reset policy options: Configuring the Drive Encryption - Windows Password Reset policy option  
**Note:** The Windows Password Reset policy option is only available in Active Directory and native policies. |
| Remote Decryption       | To configure the Remote Decryption policy option: Configuring the Drive Encryption - Remote Decryption policy option |

See “Configuring the Drive Encryption installation settings” on page 76.

**Configuring the Drive Encryption - Client Administrators policy options, for adding or editing**

Drive Encryption enables you to import a list of client administrators from a previously created installation package. Also, you can import or export list of client administrators from or into a comma separated values (CSV) file. Administrators can quickly move the client administrator’s between policies or installation packages.

**To add or edit a Drive Encryption client administrator**

1. Access the Drive Encryption policy options using an install-time, Active Directory, or native policy.

2. On the **Drive Encryption - Client Administrators** page, do one of the following:
   - To add a client administrator, click **Add**.
   - To edit an existing client administrator, select an existing client administrator, and then click **Edit**.
   - To use a list of client administrators from a previously created installation package for an Active Directory or native policy, click **Load client administrators from installation settings** from the **Action List**. Select the MSI from which you want to load the existing client administrators. See “Loading client administrators from an installation package” on page 121.
To import a list of client administrators from a CSV file, click **Import client administrators from csv** from the **Action List**, and click **Save**. See “Importing and exporting client administrators” on page 119.

To export a list of client administrators into a CSV file, click **Export client administrators to csv** from the **Action List**, and click **Save**. See “Importing and exporting client administrators” on page 119.

---

**Note:** You can modify the exported list and add more client administrators. You can also create a new csv file with client administrator's account name, password, and privileges and import the csv file. See “About creating a CSV file for client administrator accounts” on page 120.

---

3. In the **Add New Client Administrator** dialog box or the **Edit Client Administrator** dialog box, type the name of the account in the **Account Name** box.

**Note:** For upgrades: If you load client administrator accounts that were added using a software version earlier than Symantec Endpoint Encryption 11.0, under the **Password Status** column you may see the value **Re-enter** in red font. This value notifies you that you must re-enter this client administrator's password. The old password is encrypted under an older algorithm. Until you enter a new password, the client administrator cannot log on. You can enter the same password as the client administrator's current password. For more information, see the *Symantec Endpoint Encryption Upgrade Guide*.

---

4. Type the password for this client administrator account in the **Password** and **Confirm Password** boxes.

   The password must be a minimum of 2 characters and a maximum of 32 characters.

5. Select the privileges that you want to grant the client administrator. You can select **Default** to grant all of the available privileges.

6. Click **OK** to save the newly added or edited client administrator.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111. See “About client administrator privileges” on page 119. See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.
About client administrator privileges

The Management Console lets Symantec Endpoint Encryption Management Server administrators configure specific privileges while defining client administrators. This definition and configuration can happen in install-time, GPO, and native policies for Drive Encryption client computers. Client administrator privileges grant access to specific client administrator functions, such as decrypting drives and unlocking computers that missed their scheduled check-in date.

The following table describes the client administrator privileges that are available.

Table 6-3  Client administrator privileges

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User management</td>
<td>Enables the client administrator to register new users and unregister existing users.</td>
</tr>
<tr>
<td>Decrypt drives</td>
<td>Enables the client administrator to manually decrypt drives on client computers.</td>
</tr>
<tr>
<td>Extend lockout</td>
<td>Enables the client administrator to extend the amount of time left for the next required check in with the Symantec Endpoint Encryption Management Server to prevent a lockout.</td>
</tr>
<tr>
<td>Unlock</td>
<td>Enables the client administrator to unlock encrypted drives when Management Agent misses its scheduled check in with the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Default administrator</td>
<td>Enables all of the available privileges for the client administrator.</td>
</tr>
</tbody>
</table>

Importing and exporting client administrators

You can import and export your list of client administrators from a comma separated value (CSV) file. This feature lets you reuse already created client administrator names, passwords and administrative privileges.

This feature lets you quickly add large amounts of client administrator accounts into your Drive Encryption installation settings without having to manually enter each one. Your CSV file includes client administrator user names, passwords and administrative privileges.

See “About creating a CSV file for client administrator accounts” on page 120.
To import client administrators:

1. In the Management Console, go to Symantec Endpoint Encryption Software Setup > Drive Encryption.
2. In the Drive Encryption Installation Settings - Client Administrators page, in the Action List drop-down list, click Import client administrators from csv.
3. In the Choose file dialog box, browse to your CSV file.
4. Click Open.
5. In the Client Administrators Import/Export dialog box, click OK.

To export client administrators:

1. In the Management Console, go to Symantec Endpoint Encryption Software Setup > Drive Encryption.
2. In the Drive Encryption Installation Settings - Client Administrators page, in the Action List drop-down list, click Export client administrators to csv.
3. In the Choose file dialog box, browse to the location where you want to save the CSV file.
4. In the Client Administrators Import/Export dialog box, click OK.

About creating a CSV file for client administrator accounts

You can import and export your list of client administrators from a comma separated value (CSV) file. This feature enables you reuse already created client administrator names, passwords and administrative privileges.

See “Importing and exporting client administrators” on page 119.

Your CSV file must use the following format:

Account name, Password, Privileges

For example:

Admin1, mypass1, user management, decrypt drives

Note: User names and passwords are case sensitive.

You can specify privileges, separated by commas, as follows:

- User management - Allows the client administrator to register as well as unregister users from the client computer.
■ Decrypt drives - Enables the client administrator decrypt drives on the client computer.

■ Extend lockout - Enables the client administrator to extend the amount of time left for the next required check in with the Symantec Endpoint Encryption Management Server to prevent a lockout.

■ Unlock - Enables the client administrator to unlock encrypted client computers when Management Agent misses its scheduled check in with the Symantec Endpoint Encryption Management Server.

■ All - Grants the client administrator all privileges on the client computer.

Loading client administrators from an installation package

You can create multiple client installation packages and reuse your client administrators. This feature lets you quickly add large amounts of client administrator accounts into your Drive Encryption installation settings without having to manually enter each one.

You can use installation packages created from Symantec Endpoint Encryption 11.0.0 and 11.0.1 (Drive Encryption Client MSI) to load the client administrators list.

See “About client installers” on page 69.

To load client administrators from an installation:

1 In the Management Console, go to Symantec Endpoint Encryption Software Setup > Drive Encryption.

2 In the Drive Encryption Installation Settings - Client Administrators page, in the Action List drop-down list, click Load client administrators from installation.

3 In the Choose file dialog box, browse to your previously created Drive Encryption MSI installation file.

4 Click Open.

Configuring the Drive Encryption - Client Administrators policy options, for deleting

Preparing to delete client administrators

For an Active Directory or native policy, you can click Load client administrators from installation settings to load your current list of client administrators. You are prompted to select the MSI from which you want to load the administrators.
Caution: For upgrades, if you load client administrator accounts from an MSI that was generated using a software version earlier than Symantec Endpoint Encryption 11.0, under the **Password Status** column the value of **Re-enter** is displayed in red font for every client administrator. This value notifies you that you must re-enter a client administrator's password. The old password was encrypted under an older algorithm. Until you enter a new password, these client administrators cannot log on. After you delete the desired client administrators, therefore, use the edit function to change the passwords of the remaining client administrators. You can re-enter a client administrator's current password. The new passwords are encrypted with the new algorithm.

See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.

For more information, see the *Symantec Endpoint Encryption Upgrade Guide*.

**Deleting client administrators**

**To delete a Drive Encryption client administrator**

1. Access the Drive Encryption policy option using an install-time, Active Directory, or native policy.

2. On the **Drive Encryption - Client Administrators** page, select the client administrator that you want to delete. You can use Shift+click or Ctrl+click to select multiple client administrators.

3. Click **Delete**.

   **Note:** You must have at least one client administrator in the list before leaving this page.

4. On the confirmation dialog box, click **OK**.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

**Configuring the Drive Encryption - Registered Users policy options**

**To configure the authentication and the registration method for Drive Encryption users**

1. Access the Drive Encryption policy options using an install-time, Active Directory, or native policy.

2. On the **Drive Encryption - Registered Users** page, under **Authentication Method**, select an option from the **Require registered users to authenticate with** box to configure authentication method for Drive Encryption users.
(Default) To have users authenticate with a password, click a password.
To have users authenticate with a token, click a token.
To have users authenticate using either a password or a token, click password or token.

3 Under User Registration, select a user registration option to configure the user registration method for Drive Encryption users.

- (Default) To allow users to authenticate and register using a Windows user name and a Windows password or token, click Using Windows user authentication credentials.

Note: The single sign-on policy is applicable only to this type of users.

- To allow users to authenticate and register using a Windows user name and a Drive Encryption password, click Using Windows username, non-Windows password.

Note: This option is not available if you have selected either a token, or password or token, from the Require registered users to authenticate with list box.

- To allow users to authenticate and register using a Drive Encryption user name and a Drive Encryption password, click Using non-Windows username, non-Windows password.

Note: This option is not available if you have selected either a token, or password or token, from the Require registered users to authenticate with list box.

4 Click Next.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

About user registration basics for administrators

A registered user is one who is registered with Symantec Endpoint Encryption Drive Encryption. Once user registration happens, Drive Encryption notifies the server of a user account registration and Drive Encryption recognizes that user as a Drive Encryption registered user. This registration process ensures that the
registered user's credentials are recognized at the preboot authentication screen, which appears whenever that user restart the computer. Only a registered user of Drive Encryption can access an encrypted disk. You can configure user registration to happen with or without a user's intervention in one of the following ways:

- The policy administrator configures Drive Encryption to register a user account to an encrypted disk without user intervention. The user registration happens automatically when the user logs on to a computer that has Drive Encryption installed. Registration is silent and saves your time by automatically registering the user's Windows credentials when the user logs on using a valid authentication method.

- The client administrator registers a user account to an encrypted disk without user intervention.

- The policy administrator configures a user account and allows a user to self-register manually to an encrypted disk when required.

At least one user must register with Symantec Endpoint Encryption on each Windows client computer. When at least one user is registered on a client computer, all users are required to provide preboot authentication credentials to gain access to Windows. When a client computer connects to the Symantec Endpoint Encryption Management Server after the first user registers, the One-Time Password feature's authentication mode changes from Offline to Online.

**Note:** If you enable the Autologon feature on a client computer permanently, preboot authentication is disabled permanently. However, the Drive Encryption client continues to register new users’ Windows credentials automatically.

Symantec Endpoint Encryption supports both password and smart card authentication for registered users. You can use the Management Console to configure whether only one or both authentication methods are enabled. Users of both authentication methods must log off from Windows and log on again with the second authentication method to ensure that it is registered.

When a new user is registered, they are prompted to set their Drive Encryption Self-Recovery security questions, if any, and enter their answers. You can configure the number of questions that users define and that you predefine, or select a mix of user-defined and predefined questions.

See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.

See “Configuring the Drive Encryption - Registered Users policy options” on page 122.
See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 132.

See “Providing One-Time Password user assistance for legacy Symantec Endpoint Encryption clients” on page 252.

Configuring the Drive Encryption - Single Sign-On policy options

To configure the Single Sign-On policy options

1 Access the Drive Encryption policy options using an install-time, Active Directory, or native policy.

2 On the Drive Encryption - Single Sign-On page, check Enable Single Sign-On. This option is checked by default. The selection of this option lets users authenticate at preboot and directly access the client computer without authenticating at the Windows logon screen.

3 Click Next.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Drive Encryption - Self-Recovery policy options

A user can recover from a lost password without help desk assistance by correctly answering one or more questions in pre-Windows. This policy must require at least one question. Questions can be defined in two ways:

- By you, here in this policy. These questions are the predefined questions.
- By the user, during Self-Recovery setup. Typically setup takes place during user registration, but sometimes it happens after registration. These questions are the user-defined questions.
- By both you and the user. Some of the questions can be defined in this policy; the user can also define some of the questions.

Drive Encryption Self-Recovery supports the following character set:

- Uppercase: A-Z
- Lowercase: a-z
- Digits: 0-9
- All punctuation symbols on a standard US language keyboard
To configure the Self-Recovery policy options

1. Access the Drive Encryption policy option using an install-time, Active Directory, or native policy.

2. On the Drive Encryption - Self-Recovery page, check Enable Self-Recovery to enable the Drive Encryption Self-Recovery policy for the users. This option is selected by default.

3. In the Minimum answer length box, type a value from 1-99 to set the minimum number of characters that users must use when answering Drive Encryption Self-Recovery questions. The default length is seven characters.

4. In the Predefined questions boxes, type one, two, or three predefined questions. Create the administrator-defined questions that users cannot customize. These predefined questions appear when client users configure Drive Encryption Self-Recovery. This configuration requires only answers. You can redefine a maximum of three security questions. If you need to begin again to enter a question, click Clear. The following fields change, based on your actions:
   - The number that is displayed in the Number of user-defined questions required list box is dynamically updated. The update is based on how many questions you have typed in the Predefined questions boxes.
   - The Number of predefined questions box displays the number of predefined questions currently specified.
   - The Total box displays the combined total of the Number of predefined questions required and the Number of user-defined questions required.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Drive Encryption - Startup policy options

You can use the Startup policy options to set:

- The image that appears on the Drive Encryption login screen, choosing either the Symantec Endpoint Encryption logo or a custom image. The customized image is the background of the Drive Encryption login screen, and not a logo. A Microsoft Windows client booting in UEFI mode ignores the custom images. The custom images are only available for a Microsoft Windows client booting in BIOS mode.
- A customized logon message
To configure the Drive Encryption - Startup policy options

1. Access the Drive Encryption policy options using an install-time, Active Directory, or native policy.

2. In the Preboot Splash Screen section, do one of the following:
   - Click None if you do not want a startup screen to precede the preboot authentication screen.
   - (Default) Click The SEE logo to use the Symantec Endpoint Encryption default image on the startup screen.
   - Set a custom image.
     - If this policy is an install-time policy: Click A custom image. Use the Browse button to locate the path of the image.
     - Note: The Browse button is always available, even if the The SEE logo option is selected.

     Note: The image must be in the .xpm file format. You cannot rename an existing .bmp file to an .xpm file format to use it as a custom image in the Drive Encryption login screen. The .xpm image must have dimensions of 640x480 with a maximum of 14 colors. Ensure that the size of the uploaded file is not greater than 350 KB.
     - If this policy is a GPO or native policy: Click The custom image, if available, to display your previously defined image.

3. In the Text Color menu, set the color of the legal notice text that appears on the startup screen to either Black (default) or White.
   - You can skip this step if you do not want to display a startup screen or a legal notice.

4. In the Legal notice box, enter the legal notice text that you want to display on the startup screen. By default, the Legal notice box contains a standard notice from Symantec. Click Restore Default to replace your custom notice with the default notice.
   - You can skip this step if you chose not to display a startup screen.

5. In the Preboot Login Screen section, do one of the following:
   - (Default) Click The SEE logo to use the Symantec Endpoint Encryption default image on the login screen.
   - Set a custom image.
If this policy is an install-time policy: Click **A custom image**. Use the **Browse** button to locate the path of the image.

---

**Note:** The **Browse** button is always available, even if the **The SEE logo** option is selected.

---

**Note:** The image must be in the .xpm file format. You cannot rename an existing .bmp file to an .xpm file format to use it as a custom image in the Drive Encryption login screen. The .xpm image must have dimension of 640x480 with a maximum of 14 colors. Ensure that the size of the uploaded file is not greater than 350 KB.

---

If this policy is a GPO or native policy: Click **The custom image, if available**, to display your previously defined image.

6 In the **Text Color** menu, set the color of the logon message text that appears on the login screen to either **Black** (default) or **White**.

You can skip this step if you do not want to display a logon message.

7 For an install-time policy, in the **Logon Customization** section, in the **Logon Message** box, type the logon message that you want to display at startup. Click **Restore Default** to replace your custom message with the default message of, "Welcome to Symantec Endpoint Encryption."

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

---

**About the XPM image files used for the Drive Encryption preboot screens**

Symantec Endpoint Encryption Management Server lets you add custom background images for the Drive Encryption preboot startup and login screens.

**Image specifications**

Create the custom background images according to the following specifications:

- XPM files only
- Image size of 640x480
- Palette of 14 colors only. You do not have to use all 14 colors in the image
- 8-bit RGB only. You can verify that you are using 8-bit RGB by looking at the XPM header using a text editor: 8-bit values appear as one hex triplet (for example, #285A83); 16-bit values appear as two hex triplets (for example, #28285A5A8383).
Supported graphics applications
The graphics applications that support the XPM file format include:

- Windows: Blaze ImgConvert
- Mac OS X: GIMP
- UNIX or Linux: FreeBSD
- Linux: the Convert command

Best practices for color compression
Since the image is compressed when you upload it to Symantec Endpoint Encryption Management Server, use images with few colors. For example, corporate logos using only one or two colors compress to the correct size. If you upload a highly colored image such as a photograph, the image cannot compress small enough and cannot be used. If your image does not compress, no error message appears, but the image does not appear at the Drive Encryption login screen.

On systems running Mac OS X
If you use Graphic Converter on a computer running Mac OS X, changes to your color palette may occur. As when using any graphics tool, verify that the final image is what you had intended.

Editing XPM files with text editors
If you use a text editor to modify your XPM file, ensure that any 16-bit hexadecimal values are modified to 8-bit in the colors section of the file. To modify 16-bit hexadecimal values to 8-bit, drop the second hex pair so that you end up with a hex triplet. For example, from #818184848C8C, remove the second triplet (848C8C) so that you end up with #818184.

References
For more information about XPM files, see the Wikipedia entry X PixMap (http://en.wikipedia.org/wiki/X_PixMap).
Configuring the Drive Encryption - Logon History policy options

To configure the Logon History policy options

1. Access the Drive Encryption policy option using an install-time, Active Directory, or native policy.

2. On the Drive Encryption - Logon History page, check User name to allow users to see the name of the last user who logged on. The name is visible at the Symantec Endpoint Encryption preboot authentication screen. Domain is selected by default.

3. On the Drive Encryption - Logon History page, check Domain to allow users to see the domain of the last user who logged on. The domain is visible at the Symantec Endpoint Encryption preboot authentication screen. Domain is selected by default.

Note: Making previous logon information visible reduces the security of your client computers. Therefore, Symantec recommends unchecking both User name and Domain.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Drive Encryption - Encryption policy options

To configure the Drive Encryption - Encryption policy options

1. Access the Drive Encryption policy options for an install-time policy only. You cannot change Encryption options later through policies.

2. On the Drive Encryption - Encryption page, in the AES encryption strength box, click 128-bit or 256-bit to specify the AES encryption strength.

3. Under Disk Drives, select Encrypt boot disk only or Encrypt all disks to specify which disks you want to encrypt.
4 Under Advanced Options, to include the encryption of the unused disk space while encrypting the disks and partitions, check Include unused disk space when encrypting disks and partitions. This check box is selected by default. If you uncheck this check box, Drive Encryption skips the encryption of the unused disk space while encrypting the disks and partitions. A message box appears to warn you about the potential security risk that if the unused disk space is not encrypted, the data that was deleted before initial encryption may still be accessible.

5 If you want the double-write option, check Double-write sectors during encryption or decryption (May significantly increase encryption and decryption time). Every data sector is double-written during fixed disk encryption or decryption and may significantly increase encryption and decryption time.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Drive Encryption - Client Monitor policy options

To configure the Drive Encryption - Client Monitor policy options

1 Access the Drive Encryption policy options using an install-time, Active Directory, or native policy.

2 On the Drive Encryption - Client Monitor page, choose one of the two options.

■ Click Do not enforce a minimum contact period with the SEE Management Server if you do not want to enforce regular network contact. This option is selected by default.

■ Click Lock computer after to force a computer lockout. In <x> days without contact, specify the number of days during which network contact is required, from 1–365. In Warn users <x> days before locking computer, type the number of days in advance that the users are warned to connect to the network to avoid a lockout. The number of days is from 0–364.

Note: The values you type in the Lock computer after and the Warn users <x> days before locking computer boxes are validated to ensure that users are always warned before a lockout. For example, you cannot specify that the computer should be locked after 5 days without contact, but not warn the user in time. In this example you warn them of possible lockout 15 days before they are locked out. If this case were allowed, the user could run the risk of being locked out 10 days before the warning is displayed.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.
Configuring the Drive Encryption - Help Desk Recovery policy options

In Symantec Endpoint Encryption versions before 11.0, the Help Desk Recovery policy was known as the One-Time Password (OTP) policy.

To configure the Help Desk Recovery policy options

1. Access the Drive Encryption policy option using an install-time, Active Directory, or native policy.

2. On the Drive Encryption - Help Desk Recovery page, check Enable Help Desk Recovery to provide user with Help Desk Recovery assistance at preboot authentication. This option is selected by default.

3. Check Help Desk Recovery Communication Unlock to allow a user who has been locked out of their computer for a failure to communicate to regain access using the Help Desk Recovery program.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Drive Encryption - Self-Encrypting Drives policy options

The Self-Encrypting Drives policy allows Opal v2 compliant drives to be encrypted using an Opal drive's built-in hardware encryption capability. Symantec Endpoint Encryption Drive Encryption manages and secures the drives.

Note: If a drive is hardware-encrypted rather than software-encrypted, the policy options on the Drive Encryption - Encryption policy, such as the encryption strength or inclusion of unused disk space, are not applicable.

The Self-Encrypting Drives policy allows Opal v2 compliant drives to be hardware encrypted. However, in addition to a client computer having this policy enabled, the drives must meet certain conditions. For an Opal v2 compliant drive to be hardware encrypted:

- The Opal v2 compliant drive must be on the whitelist of supported drives. See the Symantec Knowledge Base article:
  List of Opal v2 Compliant Drives

- Microsoft eDrive support - Opal v2 compliant drives must have default partitions that are created during a default Microsoft Windows installation. Alternatively, if an administrator manually creates the drive partitions following a default Windows installation, the administrator must use the Microsoft Disk Manager tool or Diskpart command-line utility. When multiple partitions exist, the number of ranges must be properly mapped with the number of partitions.
If an Opal v2 compliant drive is not provisioned in Single User Mode, Drive Encryption must be able to provision it in Global Range Mode.

If hardware encryption does not take place, Opal v2 compliant drives are software encrypted by Drive Encryption.

---

**Note:** If you have existing Opal v2 compliant drives that are already software encrypted by Drive Encryption, during an upgrade to version 11.1.0 those drives are not converted automatically to drives that are hardware encrypted. You must first decrypt the drives, then apply this policy, then re-encrypt the drives. For more information, see the *Symantec Endpoint Encryption Upgrade Guide*.

---

### To configure the Self-Encrypting Drives policy option

1. Access the Drive Encryption policy option using an install-time, Active Directory, or native policy.

2. On the *Drive Encryption - Self-Encrypting Drives* page, to allow hardware encryption on Opal v2 compliant drives, check **Use hardware encryption for compatible Opal-compliant drives**.

  See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

---

### Configuring the Drive Encryption - Windows Password Reset policy option

**To configure the Windows Password Reset policy option**

1. Access the Drive Encryption policy options using an Active Directory, or native policy.

2. On the *Drive Encryption - Windows Password Reset* page, check one or more of the following options:

   - Drive Encryption Self-Recovery - Enables enable users to change their Windows password by answering their recovery questions at preboot.
   - Help Desk Recovery - Enables users to change their Windows password with Help Desk assistance.

  **Note:** The Drive Encryption - Windows Password Reset policy settings only affect the computers on which the Windows Password Reset Utility is installed.

  See “Accessing the Symantec Endpoint Encryption policy options” on page 111.
Configuring the Drive Encryption - Remote Decryption policy option

Use a Remote Decryption GPO or native policy to remotely decrypt a client computer. Once the computer is decrypted, it remains in that state. While the policy is active, no method can be used to encrypt the disk. You must reverse this policy to allow encryption.

To configure the Drive Encryption - Remote Decryption policy option

1. Access the Drive Encryption policy options using an Active Directory or native policy.

2. On the Drive Encryption - Remote Decryption page, to remotely decrypt a client computer, check Decrypt all disks and partitions. The computer is decrypted and remains in that state.

   If you uncheck this check box, the policy is reversed and the client computer can be encrypted.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Removable Media Encryption policy options - process overview

You can configure the Removable Media Encryption policy options as described in the following table.

Table 6-4 Removable Media Encryption policy options

<table>
<thead>
<tr>
<th>Removable Media Encryption policy</th>
<th>Link to configure policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access and Encryption</td>
<td>To configure the Access and Encryption policy options: Configuring the Removable Media Encryption - Access and Encryption policy options</td>
</tr>
<tr>
<td>Device and File Type Exclusions</td>
<td>To configure the Device and File Type Exclusions policy options: Configuring the Removable Media Encryption - Device and File Type Exclusions policy options</td>
</tr>
<tr>
<td>Encryption Method</td>
<td>To configure the Encryption Method policy options: Configuring the Removable Media Encryption - Encryption Method policy options</td>
</tr>
</tbody>
</table>
Table 6-4 Removable Media Encryption policy options (continued)

<table>
<thead>
<tr>
<th>Removable Media Encryption policy</th>
<th>Link to configure policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Passwords</td>
<td>To configure the Default Passwords policy options: Configuring the Removable Media Encryption - Default Passwords policy options</td>
</tr>
<tr>
<td>Portability</td>
<td>To configure the Portability policy options: Configuring the Removable Media Encryption - Portability policy options</td>
</tr>
<tr>
<td>Expired Certificates</td>
<td>To configure the Expired Certificate policy options: Configuring the Removable Media Encryption - Expired Certificates policy options</td>
</tr>
<tr>
<td>Workgroup Key</td>
<td>To configure the Workgroup Key policy options: Configuring the Removable Media Encryption - Workgroup Key policy options</td>
</tr>
</tbody>
</table>

See “Configuring the Removable Media Encryption installation settings” on page 86.

Configuring the Removable Media Encryption - Access and Encryption policy options

Use the Access and Encryption policy to define the type of read and write access that a user has to files on removable media.

If the user has both read and write access, you can further define options for:

- Encryption Format
- Automatic Encryption
- On-Demand Encryption
To configure the Removable Media Encryption - Access and Encryption policy options

1. Access the Removable Media Encryption policy option using an install-time, Active Directory, or native policy.

2. On the Removable Media Encryption - Access and Encryption page, in the Access section, do one of the following:
   - Click Do not allow access to files on removable media to deny read and write access to the files and folders that are stored on removable media, even if a user is registered to Symantec Endpoint Encryption.
   - Click Allow read-only access to files on removable media to allow registered users to read the files that are stored on removable media. If the files are encrypted, a user must provide the credentials that were used to encrypt the files to read their content. The users cannot write files to removable media.
   - Click Allow read and write access to files on removable media to allow the registered users to read and write files to removable media. When you select this option, the options for Encryption Format, Automatic Encryption, and On-Demand Encryption are available. This option is selected by default.

3. If you selected Allow read and write access to files on removable media, in the Encryption Format section, do one of the following:
   - Click SEE RME to encrypt files to removable media using the Symantec Endpoint Encryption Removable Media Encryption 11.x format. This option is selected by default.
   - Click SEE RS to encrypt files to removable media using the Symantec Endpoint Encryption Removable Storage 8.2.1 format. Select this option if your users transfer files between the computers that use the 11.x and 8.2.1 versions. Computers using either version of the software can read these files.
   - Notify your users who work with the files that they must be aware of certain precautions when working in a mixed environment. For more information, see the following sections:
     - About backward compatibility between Removable Media Encryption and Removable Storage
     - About moving files between computers using Symantec Endpoint Encryption version 11.x and 8.2.1

4. If you selected Allow read and write access to files on removable media, in the Automatic Encryption section, do one of the following:
   - Click Do not encrypt to disable the encryption of files on removable media.
■ Click **Encrypt files as per Symantec Data Loss Prevention** to use the detection and the response capabilities of Symantec Data Loss Prevention to dictate the encryption of files.

If the **Encrypt files as per Symantec Data Loss Prevention** option is selected, Removable Media Encryption encrypts files only at the direction of Symantec Data Loss Prevention. This option requires not only Symantec Data Loss Prevention, but also the Symantec Endpoint Encryption FlexResponse Plug-In for Data Loss Prevention. Contact your sales representative to obtain this software. For more details on Symantec Data Loss Prevention, refer to the *Symantec Data Loss Prevention Administration Guide* and the *Symantec Endpoint Encryption FlexResponse Plug-In Implementation Guide*.

See the knowledge base article:
Installation of Flex Response plug-in on Removable Media Encryption client systems for DLP-based Encryption

■ Click **Encrypt new files** to automatically encrypt all files newly added to removable media. This option is selected by default.

---

**Note:** To exclude multimedia files or certain file types from automatic encryption, you can go to the **Device and File Type Exclusions** page and choose more options.

■ Click **Allow users to choose** if you want to let the users choose whether or not to automatically encrypt new files. Under the **Allow users to choose** option, select the default behavior that you want to happen if your users do not make a choice. Choose either **Default to encrypt new files**, or **Default to do not encrypt**.

5 If you selected **Allow read and write access to files on removable media**, in the **On-Demand Encryption** section, you can:

■ Check **Users can right-click to encrypt existing files on removable media** to provide users with the ability to encrypt files on removable media using a right-click menu. This option is selected by default.

■ Check **Users can right-click to decrypt existing files on removable media** to provide users with the ability to decrypt files on removable media using a right-click menu.

---

**Note:** If **Encrypt files as per Symantec Data Loss Prevention** is selected, Symantec recommends unchecking both options.
About backward compatibility between Removable Media Encryption and Removable Storage

If your users move files between computers using the Symantec Endpoint Encryption 11.x version and the 8.2.1 version, you must select the SEE RS Encryption Format option. Otherwise, if your users edit or write a file onto removable media from a computer using the 11.x version and the Encryption Format is SEE RME, their files are unreadable on the computers using the 8.2.1 version. Make sure that this Encryption Format policy option is active on their client computer before they start working with their Removable Storage 8.2.1 files.

About moving files between computers using Symantec Endpoint Encryption version 11.x and 8.2.1

You may have a mixed environment with computers using the Symantec Endpoint Encryption Removable Media Encryption 11.x version and Symantec Endpoint Encryption Removable Storage 8.2.1 version. When your users move files between these computers, advise them that the credentials they use to encrypt and decrypt files must exist on both computers. Examples of some circumstances that can cause credentials to differ are:

- The computer using the 8.2.1 version encrypts files to multiple certificates. The computer using the 11.x version encrypts files to one certificate.

- The default credentials that are set on one computer may not be the same default credentials that are set on the other computer. Default credentials are not immediately visible; the user does not receive a prompt for a password or certificate. They must be aware of which credentials are actively applied during encryption. They need those same credentials for decryption.

About working with Symantec Removable Media Encryption Burner Application

If you have computers running both Symantec Endpoint Encryption version 11.x and 8.2.1, the same conditions that apply to removable media apply to CDs, DVDs, and Blu-ray Discs. Advise your Removable Media Encryption Burner Application users that when they encrypt and burn files, they must take the precautions that are discussed in these sections:

About backward compatibility between Removable Media Encryption and Removable Storage

About moving files between computers using Symantec Endpoint Encryption version 11.x and 8.2.1

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.
Configuring the Removable Media Encryption - Device and File Type Exclusions policy options

For the device exclusions option, you must know the vendor ID and product ID of a device. A number of free tools, such as the Symantec Endpoint Encryption Device Control Auditor, can be used to obtain these IDs from your chosen device(s). Note these exceptions:

■ Memory cards - Most tools are incapable of obtaining the vendor ID and product ID of flash memory cards that can be inserted into card readers. Exempt the card reader and the flash memory cards are also exempted, as long as they are inserted into the exempted card reader.

■ eSATA drives - eSATA hard drives do not contain a vendor ID or product ID and, therefore, they cannot be exempted.

To configure the Removable Media Encryption - Device and File Type Exclusions policy option

1. Access the Removable Media Encryption policy option using an install-time, Active Directory, or native policy.

2. On the Removable Media Encryption - Device and File Type Exclusions page, set the options as described.

3. In the Exemption for Multimedia Files section, check Exclude multimedia files from automatic encryption to exclude certain files from automatic encryption. Check one or more of the check boxes according to the type of multimedia file formats you want to exclude from encryption:
   - Audio
     See “Audio file types excluded” on page 289.
   - Video
     See “Video file types excluded” on page 292.
   - Image
     See “Image file types excluded” on page 296.

4. In the File Types Exclusion section, check Exclude file types extensions from automatic encryption (comma separated), to exclude certain file types. In the input box, type the file type extensions. Examples of extensions include .jpeg and .exe.

5. In the Device Exclusions section, check Exclude these removable media encryption devices from encryption to exempt specific devices from automatic encryption. Do one of the following to exempt removable media devices from encryption:
To exempt a specific device from a vendor, enter the vendor ID, product ID, and an optional description in the fields provided.

To exempt all the devices from a vendor, enter the vendor ID in the Vendor ID box and the wildcard character * in the Product ID box. Optionally, you can also include a description in the Description (Optional) box.

**Note:** Apple devices are exempted by default.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

### Configuring the Removable Media Encryption - Encryption Method policy options

To configure the Removable Media Encryption - Encryption Method policy options

1. Access the Removable Media Encryption policy options using an install-time, Active Directory, or native policy.

2. On the **Removable Media Encryption - Encryption Method** page, do one of the following:
   - To restrict the encryption method to a password, click **A password**. This option is selected by default.
   - To restrict the encryption method to a certificate, click **A certificate**.
   - To let users choose to encrypt with a password, certificate, or both, click **A password and/or certificate**.

**Note:** If a device session default password is enabled on the Default Passwords panel, and the Encryption Method allows only certificates, the Default Passwords policy overrides this policy.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

### Configuring the Removable Media Encryption - Default Passwords policy options

Use the Defaults Passwords policy to define whether users can set a default password, up to two session passwords, or a device session password. If these passwords are set, the number of prompts users receive each time they encrypt and decrypt a file or folder is reduced.
To configure the Removable Media Encryption - Default Passwords policy options

1 Access the Removable Media Encryption policy option using an install-time, Active Directory, or native policy.

2 On the Removable Media Encryption - Default Passwords page, in the Default Password section, do one of the following:
   - To allow users to set a default password, click Allow users to set a default password. This option is chosen by default.

   **Note:** To allow users to set session passwords, you must let them set a default password.

   - To apply password aging to default passwords, check Apply password aging to Removable Media Encryption default passwords. This option ensures that users set default passwords that conform to the restrictions that you define. These restrictions are specified in the Maximum Password Age and Password History sections of the Management Agent Password Authentication policy. These restrictions set expiration dates and restrict password reuse.

   - To prevent users from setting a default password, click Do not allow users to set a default password.

   **Note:** If you do not allow users to set a default password, the Session Passwords section becomes unavailable and the Device Session Password section becomes available.

3 If the Session Passwords section is available, take one of the following actions.
   - To allow users to set session passwords, click Allow users to set session passwords. This option is chosen by default.

     If you allow session passwords, choose the session password expiration method:

     - To permanently expire (delete) session passwords at the end of each Windows session, click Delete session passwords at the end of every Windows session.

     - To temporarily expire (deactivate) session passwords at the end of each Windows session, click Deactivate session passwords at the end of every Windows session, but allow them to persist across every Windows session. The passwords remain on a user's computer, but...
To apply password aging to session passwords, click **Apply password aging to session passwords**. This option ensures that users set session passwords that conform to the restrictions that you define. These restrictions are defined in the **Maximum Password Age** and **Password History** sections of the Management Agent Password Authentication policy. These restrictions set expiration dates and restrict password reuse.

To prevent session passwords from expiring, click **Do not delete or deactivate session passwords**. This option is chosen by default.

To prevent users from setting session passwords, click **Do not allow users to set session passwords**.

If the **Device Session Password** section is available, take one of the following actions:

- To allow users to set a device session password for each removable device that is connected to a client computer, click **Allow users to set a device session password for each inserted removable media encryption device while it is currently connected**.

  **Note:** Device session passwords are useful in a kiosk environment.

  **Note:** If you enable the use of device session passwords, Removable Media Encryption overrides the Encryption Method policy, if that policy allows only certificates. Also, Removable Media Encryption ignores any Recovery Certificate policy.

  To prevent users from setting a device session password, click **Do not allow users to set a device session password for each removable device**. This option is chosen by default.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

### Configuring the Removable Media Encryption - Recovery Certificate policy options

The Recovery Certificate policy only applies to computers on which write access and encryption are enabled for removable media devices. Ensure that the Recovery
Certificate does not contain the private key and possesses the mandatory key usage.

**Note:** If you enable the use of device session passwords on the Default Passwords panel, Removable Media Encryption ignores the Recovery Certificate policy.

### To configure the Recovery Certificate policy options

1. Access the Removable Media Encryption policy options using an install-time, Active Directory, or native policy.

2. On the **Removable Media Encryption - Recovery Certificate** page, select one of the two options:
   - Click **Do not encrypt files with a recovery certificate** if you do not want to include a copy of the recovery certificate in the client installation package or policy. Removable Media Encryption, therefore, does not use a recovery certificate to encrypt files, in addition to the credentials that the user provides. This option is selected by default.
   - Click **Encrypt files with a recovery certificate** if you want to include a copy of the recovery certificate in the client installation package or policy. After you select this option, Symantec Endpoint Encryption prompts you to locate a PKCS#7 (P7B) format certificate file on your system. When you select a certificate, the details of the certificate appear in the **Select Certificate** dialog box. Before you confirm the addition of the certificate to the client installer or policy, view the certificate. After you confirm the certificate, the **Issued By** and **Serial Number** information appears on the Removable Media Encryption - Recovery Certificate panel. To select a different certificate file, click **Change certificate**.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

See “Best practices for using a recovery certificate” on page 143.

### Best practices for using a recovery certificate

Symantec recommends the following best practices for using a recovery certificate:

- Be sure to create and use a long-life recovery certificate. This means that the recovery certificate should not expire within a year but should be valid for at least five years.

- The users are not notified about the expiry of the recovery certificate. Therefore, ensure that you track the expiry of the recovery certificate where you and the users can see it, such as on a group calendar. You can create a
Configuring the Removable Media Encryption - Portability policy options

The Portability policy has the following options:

- Removable Media Access Utility
- Self-Decrypting Archive

To configure the Portability policy options

1. Access the Removable Media Encryption policy options using an install-time, Active Directory, or native policy.

2. On the Removable Media Encryption - Portability page, in the Access Utility section, do the following:
   - Check Copy the Removable Media Access Utility for Windows to removable media to write automatically to removable media the Removable Media Access Utility that runs on Microsoft Windows computers.
   - Check Copy the Removable Media Access Utility for Mac OS X to removable media to write automatically to removable media the Removable Media Access Utility that runs on Macintosh computers.

3. In the Self-Decrypting Archive section, check Allow users to save files as password encrypted self-decrypting archive to permit users to create self-decrypting archives.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.
Configuring the Removable Media Encryption - Expired Certificates policy options

To configure the Removable Media Encryption - Expired Certificates policy option

1. Access the Removable Media Encryption policy using an install-time, Active Directory, or native policy.

2. On the Removable Media Encryption - Expired Certificates page, check Users can use expired certificates to encrypt files so that the user can encrypt a file using their expired certificate. If you uncheck this option, the user cannot use the expired certificate for file encryption.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Removable Media Encryption - Workgroup Key policy options

A workgroup key is shared among all Removable Media Encryption users of the target computers to enable file sharing. The workgroup key setting is available as an Active Directory policy or native policy, but not as an install-time policy.

To enable distribution of Removable Media Encryption workgroup key to your Active Directory computers, you must enable Windows authentication. To enable Windows authentication, ensure that you do the following:

- Select the Windows Authentication security server role from the Add Roles and Feature Wizard available in the Server Manager.

- Select the Enable Windows Authentication check box available in the Symantec Endpoint Encryption Web Server Configuration page.

If you want to distribute the workgroup key using Group Policy Objects (GPO) to Removable Media Encryption client computers, Symantec strongly recommends you to refer the Symantec knowledge base article, https://support.symantec.com/en_US/article.DOC9126.html. This knowledge base article provides information on how to configure your Active Directory conforming to the location of the Symantec Endpoint Encryption Management Server and Removable Media Encryption endpoints in an Active Directory forest.

**Note:** The Removable Media Encryption workgroup key defined in a GPO linked at site-level is not supported. The Symantec Endpoint Encryption Management Server ignores Windows Management Instrumentation (WMI) filters applied to GPO while distributing the workgroup key to Removable Media Encryption endpoints.
To configure the Removable Media Encryption - Workgroup Key policy option

1. Access the Removable Media Encryption policy options using an Active Directory or native policy.

2. On the Removable Media Encryption – Workgroup Key page, to enable this option, click Encrypt and decrypt files with this workgroup key.

3. Fill the key box automatically or manually.
   - To fill the key box automatically with a randomly generated number, click Generate new key.
   - To fill the key box manually, type or paste a key, whose value is random, 64 digits, in hexadecimal format, with lowercased alphanumeric characters.

4. Optionally type some descriptive text for this key in the Memo field.

Note: This text appears on the Resultant Set of Policy (RSoP) report.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.

Configuring the Mac FileVault Client policy options - process overview

You can configure the Mac FileVault Client install-time policy options for Symantec Endpoint Encryption for FileVault as described in the following table.

Note: No GPO or native policy exists to update the install-time policy settings.

### Table 6-5 Mac FileVault Client policy options

<table>
<thead>
<tr>
<th>Mac FileVault Client policy options</th>
<th>Link to configure the policy options</th>
</tr>
</thead>
</table>
| Introduction                        | To configure the Introduction policy options:  
|                                     | Configuring the Mac FileVault Client - Introduction policy options |
| Institutional Recovery Key          | To configure the Institutional Recovery Key policy options:  
|                                     | Configuring the Mac FileVault Client - Institutional Recovery Key policy options |
Table 6-5  Mac FileVault Client policy options (continued)

<table>
<thead>
<tr>
<th>Mac FileVault Client policy options</th>
<th>Link to configure the policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>To configure the Communication policy options:</td>
</tr>
<tr>
<td></td>
<td>Configuring the Mac FileVault Client - Communication policy options</td>
</tr>
</tbody>
</table>

See “Creating a Symantec Endpoint Encryption for FileVault installation package” on page 97.

Configuring the Mac FileVault Client - Introduction policy options

About Apple FileVault 2 (FileVault) and Symantec Endpoint Encryption Management Server

When you enable FileVault on your Macintosh computer, the Symantec Endpoint Encryption for FileVault client concurrently generates a unique Personal Recovery Key. This Personal Recovery Key is specific to each Macintosh computer. A Macintosh computer is uniquely identified with a serial number. The Symantec Endpoint Encryption for FileVault client sends the serial number of a Macintosh computer along with the Personal Recovery Key to the Symantec Endpoint Encryption Management Server. Symantec Endpoint Encryption Management Server saves the serial number and the Personal Recovery key in the database and uses them for user access recovery.

You can encrypt the disks on a client computer using FileVault. Using the Symantec Endpoint Encryption Management Server, you can track the various activities of the client computers. Using the Help Desk Recovery program, you can provide recovery support to the client users when they lose their password or are locked out at preboot.

About Mac FileVault Client installation wizard

You can use the Mac FileVault Client installation wizard to create an installer for Symantec Endpoint Encryption for FileVault. You can distribute this installer to your organization’s Macintosh computers so that you can manage the Apple encryption software that is installed on those systems.

There are no policy options on the Mac FileVault Client - Introduction page to configure. This page lists the version numbers of the Apple Mac OS X operating systems for which you can create the Symantec Endpoint Encryption for FileVault installation package.
To view the Mac FileVault Client - Introduction policy option

- On the Create Mac OS X Installer - Introduction page, read about the supported operating systems, then click Next.

Configuring the Mac FileVault Client - Institutional Recovery Key policy options

FileVault supports an Institutional Recovery Key (IRK) in addition to the Personal Recovery Key. Institutional Recovery Key is a single key that can be used to unlock any system in the company or a group. You can also maintain an enterprise-wide Institutional Recovery Key that your department can use to decrypt any system when you are in physical possession of that system. Apple has an article on the creation and use of institutional recovery keys. For more information, refer to the Apple user community and knowledgebase. You can create the Institutional Recovery Key by following the instructions on the Apple site.

The Institutional Recovery Key is an optional key that can be uploaded to the Symantec Endpoint Encryption Management Server, and only the public key of Institutional Recovery Key is included in the install-time policy.

When a user installs the Symantec Endpoint Encryption for FileVault installation package with the Institutional Recovery Key certificate included in the policy, then the Institutional Recovery Key is included in the FileVault setup.

To configure the Mac FileVault Client - Institutional Recovery Key policy option

1. On the Create Mac OS X Installer - Institutional Recovery Key page, to include an Institutional Recovery Key certificate in the install-time policy check Use an Institutional Recovery Key. This option is checked by default.

2. Click Change Key to locate the path of the Institutional Recovery Key certificate, and select it.

Note: The Change Key button is available only when you check Use an Institutional Recovery key.

The Common Name of the issuer must be ‘FileVault Recovery Key’ and Signature Algorithm must be ‘SHA-1 with RSA Encryption’.
3. After you select the Institutional Recovery Key certificate, the name of the provider and the serial number of the Institutional Recovery Key certificate appear in the **Issued By** and **Serial** boxes on the **Create Mac OS X Installer - Institutional Recovery Key** page. To select a different Institutional Recovery Key certificate, click **Change Key**.

Symantec Endpoint Encryption Management Server saves the newly selected or changed Institutional Recovery Key certificate in the database and uses it for user-access recovery.

4. Click **Next**.

### Configuring the Mac FileVault Client - Communication policy options

Specifies the interval at which the recipient Macintosh computers attempt to make contact with Symantec Endpoint Encryption Management Server. When communication is established between the client computers and the server, the client sends the client information, such as the serial number of the Macintosh computer, along with the Personal Recovery Key.

**To configure the Mac FileVault Client - Communication policy option**

1. On the **Create Mac OS X Installer - Communication** page, in the **Communication** section, do the following:

   - In the **Send status updates every <x> minutes** box, enter the interval, in minutes at which Symantec Endpoint Encryption for FileVault running on the Macintosh computer reports any changes in the status data. The changes are reported to the selected Management Server. The default value is 60 minutes.

2. In the **Communication information** section:

   The following fields are prefilled as follows:

   - **Connection Name** displays the name of Symantec Endpoint Encryption Management Server.

   - **Server** displays the URL of the Web service running on the selected Management Server, including its NetBIOS name or FQDN and port number.

   - **Name** and **Domain** displays the name and domain of the IIS client account.

   - **Certificate Hash** displays the details of the server certificate, only if the server connection is secure.

   Do the following:

   - In the **Password** box, type the password of the IIS client account.
3 Click Finish.
4 In the Save Mac Package dialog box, navigate to the location where you want to save the Symantec Endpoint Encryption for FileVault installation package.
5 If required, change the default Symantec Endpoint Encryption for FileVault package name.
6 Click Save to create the Symantec Endpoint Encryption for FileVault installer with the administrative policies you have configured at your desired location.

### Configuring the BitLocker Client policy options - process overview

You can configure the BitLocker Client options for Symantec Endpoint Encryption for BitLocker as described in the following table.

<table>
<thead>
<tr>
<th>BitLocker Client policy</th>
<th>Link to configure the policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption and Authentication</td>
<td>To configure the Encryption and Authentication policy options:</td>
</tr>
<tr>
<td></td>
<td>Configuring the BitLocker Client - Encryption and Authentication policy options</td>
</tr>
<tr>
<td>Client Monitor</td>
<td>To configure the BitLocker Client Monitor policy options:</td>
</tr>
<tr>
<td></td>
<td>Configuring the BitLocker Client - Client Monitor policy options</td>
</tr>
</tbody>
</table>

See “Creating a Symantec Endpoint Encryption Client installation package” on page 72.

### Configuring the BitLocker Client - Encryption and Authentication policy options

Microsoft BitLocker provides encryption at the block level for volumes.

**To configure the BitLocker Client - Encryption and Authentication policy options**

1. Access the BitLocker Client policy options using an install-time, Active Directory, or native policy.
2. On the BitLocker – Encryption and Authentication page, select an encryption or a decryption policy option.
3 For the encryption policy option, do the following to select the encryption and the authentication policies:

■ To encrypt all volumes on a client computer, select **Encrypt all volumes**. This option is checked by default.

■ In the **Encryption Method** section, you must select an encryption strength; you may select an encryption mode. For all Windows systems, select 128-bit or 256-bit in the **AES encryption strength** box to specify the AES encryption strength. For systems running Windows 10 version 1511 and later, optionally also select **Prefer the XTS-AES encryption mode, if available**. The AES encryption strength that you selected is applied.

■ In the **Authentication Method** section, select an option to specify how users gain access to the client computer. Do one of the following:

■ To have users authenticate with TPM, click **Trusted Platform Module (TPM)**. User intervention or credentials are not required to gain access to the client computer.

■ To have users authenticate with TPM and a PIN, click **TPM and PIN**. This option is selected by default. The PIN length must be 4 - 20 digits.

■ To use the password authentication method for the client computers that do not have TPM chip, or do not have TPM in a ready-to-use state, click **Fall back to password if TPM is unavailable**. This option is selected by default. The password length must be 8 - 99 characters. This policy option is supported on computers having operating system Windows 8 or later installed.

4 For the decryption policy option, select **Decrypt all volumes** to decrypt all the volumes on a client computer. Symantec Endpoint Encryption for BitLocker first decrypts all of the data volumes and then decrypts the boot volume.

**Configuring the BitLocker Client - Client Monitor policy options**

1 Access the BitLocker Client policy options using an install-time, Active Directory, or native policy.

2 On the **BitLocker Client - Client Monitor** page, choose one of the two options that you want to apply to a computer with Symantec Endpoint Encryption for BitLocker installed:

■ Click **Do not enforce a minimum contact period with the SEE Management Server** if you do not want to enforce regular network contact. This option is selected by default.
Click **Lock computer after** to force a computer lockout. In **<x> days without contact**, specify the number of days during which network contact is required, from 1 - 365. In **Warn users <x> days before locking computer**, type the number of days in advance that the users are warned to connect to the network to avoid a lockout. The number of days is from 0 - 364.

**Note:** The values you type in the **Lock computer after** and the **Warn users <x> days before locking computer** boxes are validated to ensure that users are always warned before a lockout. For example, if you warn them of possible lockout 15 days before locking the computer, but you lock the computer after only 5 days, then the user runs the risk of being locked out 10 days before the warning is displayed.

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.
Creating and managing Symantec Endpoint Encryption GPO and native policies

This chapter includes the following topics:

■ About policy creation and management
■ Managing GPOs - process overview
■ Creating and editing GPOs or restoring installation settings
■ Managing native policies - process overview
■ Creating and editing native policies
■ Managing Symantec Endpoint Encryption policies on virtual desktops

About policy creation and management

Policies define certain behaviors of users and client computers in Symantec Endpoint Encryption. The first sets of policies that you create are the installation policies, which result in the creation of MSI packages.

Once installation policies are deployed and installed, you can change most of the settings, as needed. To make changes, define and apply Active Directory Group Policy Object (GPO) policies or native policies. Policy settings take precedence over installation settings on a client. While both types of policies contain identical options, you create and edit GPOs and native policies differently.
See “Managing GPOs - process overview” on page 154.
See “Managing native policies - process overview” on page 158.

Managing GPOs - process overview

Use the Group Policy Editor to create and edit your GPOs.

Table 7-1  Process for managing GPOs

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create or edit a GPO, or reset the policy to its installation settings</td>
<td>Create a new GPO or edit an existing GPO. To view the available policy options:</td>
</tr>
<tr>
<td></td>
<td>See “About configuring the Symantec Endpoint Encryption policy options” on page 109.</td>
</tr>
<tr>
<td></td>
<td>To create or edit a policy, or restore the installation settings:</td>
</tr>
<tr>
<td></td>
<td>See “Creating and editing GPOs or restoring installation settings” on page 154.</td>
</tr>
<tr>
<td>Deploy the policy</td>
<td>Deploy GPOs using the Microsoft Group Policy Editor or force an immediate policy update from the client.</td>
</tr>
<tr>
<td></td>
<td>See “Deploying GPOs - process overview” on page 166.</td>
</tr>
</tbody>
</table>

Creating and editing GPOs or restoring installation settings

About policy changes

In Symantec Endpoint Encryption Management Server versions earlier than 11.0, the Help Desk Recovery policy (previously known as One-Time Password (OTP)), the Drive Encryption Self-Recovery policy (previously known as Authenti-Check), and the Single Sign-On policy were user-based. In Symantec Endpoint Encryption Management Server version 11.x, the Help Desk Recovery and Drive Encryption Self-Recovery policy options are computer-based. Therefore, when you upgrade Symantec Endpoint Encryption Management Server from versions earlier than 11.0 to an 11.x version, you must create new computer-based policies for Help Desk Recovery and Drive Encryption Self-Recovery.

In Symantec Endpoint Encryption Management Server version 11.x, the Single Sign-On policy option is computer-based. Therefore, when you upgrade Symantec
Endpoint Encryption Management Server from versions earlier than 11.0 to an 11.x version, you must create a new computer-based policy for Single Sign-On.

When you apply a policy to a Symantec Endpoint Encryption client version earlier than 11.0, any policy option that is no longer supported in version 11.x is reset to its default value. These older options continue to appear on the version 11.x policy panels, but they are grayed out and cannot be changed. When you modify the active options and then deploy the policy to earlier clients, the grayed-out options are set to their original default values.

**About creating GPOs to distribute client installation packages**

To use GPOs to distribute your client installation packages, you must create a separate GPO for each MSI package if you want to deploy MSI packages on both 32-bit and 64-bit computers.

**Creating or editing GPOs**

To create or edit a GPO or restore installation settings

1. Expand the Group Policy Management snap-in.
2. Expand your forest.
3. Expand **Domains**, and then expand the specific domain.
4. Expand **Group Policy Objects**.
5. To create a new GPO, right-click **Group Policy Objects** and select **New**. Alternatively, to edit a GPO, right-click the GPO and select **Edit**.
6. In the Group Policy Management Editor, to identify the type of policy that you want to create, do one of the following:
   - Expand **Computer Configuration**.
   - Expand **User Configuration**.
7. Expand **Policies**.
8. Expand **Software Settings**.
9. Expand **Symantec Endpoint Encryption**.
10. Expand **Management Agent, Drive Encryption, Removable Media Encryption**, or **BitLocker Client** as appropriate.
11. Select the policy that you want to modify, and then click **Change these settings**.

   To see the options for your selected policy, refer to the User Configuration or Computer Configuration table.
Perform the appropriate action:

- For a new or a modified policy, select the new settings. Click away from the panel to validate your entries and make any corrections.

- To reset the policy to its original settings, click **Restore the installation settings**. When this policy is applied to the client computer, the computer disregards any existing policies. The computer returns to the settings that were specified in the client installation package.

Click **Save**.

Add or edit another policy or close the Group Policy Management Editor window.

**Computer Configuration:**

**Software Settings**

**Management Agent**

See “Configuring the Management Agent - Password Authentication policy options” on page 113.

See “Configuring the Management Agent - Communication policy options” on page 115.

**Drive Encryption**

See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.

See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.

See “Configuring the Drive Encryption - Registered Users policy options” on page 122.

See “Configuring the Drive Encryption - Single Sign-On policy options” on page 125.

See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.

See “Configuring the Drive Encryption - Startup policy options” on page 126.

See “Configuring the Drive Encryption - Logon History policy options” on page 130.

See “Configuring the Drive Encryption - Client Monitor policy options” on page 131.

See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 132.
Computer Configuration: 
Software Settings

See “Configuring the Drive Encryption - Self-Encrypting Drives policy options” on page 132.

See “Configuring the Drive Encryption - Windows Password Reset policy option” on page 133.

See “Configuring the Drive Encryption - Remote Decryption policy option” on page 134.

Removable Media Encryption


See “Configuring the Removable Media Encryption - Device and File Type Exclusions policy options” on page 139.

See “Configuring the Removable Media Encryption - Encryption Method policy options” on page 140.

See “Configuring the Removable Media Encryption - Default Passwords policy options” on page 140.


See “Configuring the Removable Media Encryption - Workgroup Key policy options” on page 145.

See “Configuring the Removable Media Encryption - Portability policy options” on page 144.

See “Configuring the Removable Media Encryption - Expired Certificates policy options” on page 145.

BitLocker Client

See “Configuring the BitLocker Client - Encryption and Authentication policy options” on page 150.

See “Configuring the BitLocker Client - Client Monitor policy options” on page 151.

Verifying policy application

After you deploy policies, you can verify their intended application by creating and viewing a Group Policy Report.
Managing native policies - process overview

To create or edit a native policy, use the Symantec Endpoint Encryption Native Policy Manager.

### Table 7-2  Process for creating and editing native policies

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create or select a native policy</td>
<td>Create a native policy by using the Symantec Endpoint Encryption Native Policy Manager snap-in. See “Creating and editing native policies” on page 158.</td>
</tr>
<tr>
<td>Deploy a native policy</td>
<td>Deploy a native policy by creating Symantec Endpoint Encryption Managed Computers groups, and then assigning policies to them. The client computers check in with Symantec Endpoint Encryption Management Server to receive their policies or you can force the update on the client computer. See “Deploying native policies - process overview” on page 168.</td>
</tr>
</tbody>
</table>

Creating and editing native policies

### About creating and editing native policies

When you apply a policy to a Symantec Endpoint Encryption client version earlier than 11.0, any policy setting that is no longer supported in version 11.x is reverted to its default value. These older settings continue to appear on the version 11.x policy panels, but they are grayed out and cannot be changed. When you modify the active settings in the panel and then deploy the policy to the earlier Symantec Endpoint Encryption clients, the grayed-out settings are reverted to their original default values. For native policies, be aware that when you deploy an updated native policy to earlier versions of the Symantec Endpoint Encryption clients, all policy settings that are no longer configurable in Symantec Endpoint Encryption Management Server are reset for all product features.

### Creating or selecting native policies

**To create a new native policy**

1. In the Management Console, right-click **Symantec Endpoint Encryption Native Policy Manager**.
2. Select **Create New Policy** to open the SEE - Native Policy dialog box.
3 In the **New Policy** field, type a name for your policy. Keep in mind the following restrictions and behavior:
- Names must be unique.
- Names are not case-sensitive.
- Spaces inserted before or after the name are deleted.

4 Click **OK**.

5 Set the options on one or more of the policy panels to create this native policy:

See the section called “Configuring native policies” on page 159.

**To select an existing native policy**

1 Expand **Symantec Endpoint Encryption Native Policy Manager**.
2 Locate the name of the policy that you want to edit and left-click to select it.
3 Set the options on one or more of the policy panels to update this native policy:

See the section called “Configuring native policies” on page 159.

**Configuring native policies**

After you create or select an existing native policy, in the Management Console the Native Policy Manager displays the policy panels in the right pane. The panels appear sequentially in a single wizard for the Management Agent, the Drive Encryption feature, the Removable Media Encryption feature, and the BitLocker Encryption feature. You must click through every panel of every feature in the wizard to create one native policy.

**Note:** Drive Encryption and BitLocker Encryption cannot co-exist on a client; only one component can be installed.

To see instructions for configuring any policy option, click the appropriate link in the table.

Navigate the native policy wizard as follows:

- To proceed to the next panel, click **Next**.
- To review previous panels, click **Back**. Your settings on the current panel are saved.
- To create your native policy, on the final panel click **Finish**. To close the confirmation message, click **OK**.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Link to policy options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Agent</td>
<td>See “Configuring the Management Agent - Password Authentication policy options” on page 113.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Management Agent - Communication policy options” on page 115.</td>
</tr>
<tr>
<td>Drive Encryption</td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for adding or editing” on page 117.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Client Administrators policy options, for deleting” on page 121.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Registered Users policy options” on page 122.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Single Sign-On policy options” on page 125.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Self-Recovery policy options” on page 125.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Startup policy options” on page 126.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Logon History policy options” on page 130.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Client Monitor policy options” on page 131.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Help Desk Recovery policy options” on page 132.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Self-Encrypting Drives policy options” on page 132.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Windows Password Reset policy option” on page 133.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Drive Encryption - Remote Decryption policy option” on page 134.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Removable Media Encryption - Device and File Type Exclusions policy options” on page 139.</td>
</tr>
</tbody>
</table>
Managing Symantec Endpoint Encryption policies on virtual desktops

About creating and managing policies on virtual desktops

You can use Citrix XenDesktop (version 7.1) to deploy and manage your Symantec Endpoint Encryption policies on the clients that are deployed on virtual desktops, known as machine catalogs.

To deploy and manage your policies in this virtual environment:

- Create a master image to be used as the parent image of the machine catalogs that you provision.
- For new machine catalogs, deploy the Symantec Endpoint Encryption client software (Symantec Endpoint Encryption Management Agent and Symantec Endpoint Encryption Removable Media Encryption only) to the master image, and then create the machine catalogs.
For existing machine catalogs, deploy the Symantec Endpoint Encryption client software to the master image, and then update the machine catalog.

In the Management Console on Symantec Endpoint Encryption Management Server, view the master image and the machine catalogs as individual client computers.

Deploy the Active Directory GPOs and native policies to the master image and machine catalogs.

**Deploying GPO and native policies to virtual desktops**

Deploy GPOs to machine catalogs by setting up the machine catalogs and Symantec Endpoint Encryption Management Server in the same domain.

Deploy native policies to machine catalogs using Symantec Endpoint Encryption Managed Computers groups by setting up the machine catalogs and Symantec Endpoint Encryption Management Server in different domains.

**Managing Symantec Endpoint Encryption policies independently of Citrix XenDesktop policies**

When you create new machine catalogs using a master image, the machine catalogs have the same policy settings as that of the master image. However, you can also manage the Symantec Endpoint Encryption policies on the machine catalogs independently of the master image.

To manage the policies on the clients independently of the master image:

- For GPOs, group the clients into different organizational units (OUs) and deploy policies specific to each group.

- For native policies, use the Symantec Endpoint Encryption Users and Computers snap-in and deploy policies specific to each managed computers group.

**Enabling removable media device connection in a virtual environment**

If you deploy Removable Media Encryption to your virtual desktops, your users must be able to work with removable devices.

To allow users to connect removable media devices to the machine catalogs

- Enable the USB redirection policy in Citrix XenDesktop

See “About policy creation and management” on page 153.

See “Managing GPOs - process overview” on page 154.

See “Managing native policies - process overview” on page 158.
See “Deploying GPOs - process overview” on page 166.
See “Deploying native policies - process overview” on page 168.
Creating and managing Symantec Endpoint Encryption GPO and native policies
Managing Symantec Endpoint Encryption policies on virtual desktops
Deploying Symantec Endpoint Encryption GPO and native policies

This chapter includes the following topics:

- Deploying GPOs - process overview
- About Active Directory Computers
- Deploying GPOs
- Forcing GPO updates
- About GPO priority sequence
- About GPO assignment verification
- Deploying native policies - process overview
- About Symantec Endpoint Encryption Managed Computers groups
- Creating Symantec Endpoint Encryption Managed Computers groups
- Moving computers from a Symantec Endpoint Encryption Managed Computers group to another group
- Deleting a computer from a managed computer group
- Searching for specific computers
- About wildcard search characters
- About assigning native policies
Deploying GPOs - process overview

You can deploy GPOs by using the Microsoft Group Policy Management Console (GPMC) snap-in. You can also force the update from the client computer.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy a GPO using the Microsoft Group Policy Management Console snap-in</td>
<td>To deploy GPO: See “Deploying GPOs” on page 167.</td>
</tr>
<tr>
<td>(Optional) Deploy a GPO manually</td>
<td>To force a GPO update from the client computer: See “Forcing GPO updates” on page 167.</td>
</tr>
<tr>
<td>Consider the order of precedence in which your policies are applied</td>
<td>To learn about GPO order of precedence: See “About GPO priority sequence” on page 168.</td>
</tr>
</tbody>
</table>

About Active Directory Computers

Active Directory policies are assigned to individual computers, subgroups, or the groups that are located within the Active Directory Computers container. This container is located in the Management Console Symantec Endpoint Encryption Users and Computers snap-in.

When Active Directory synchronization is enabled, the computers in the Active Directory forest or domain are listed in the Active Directory Computers container. You cannot move or modify the computer and the user objects that are located within the Active Directory Computers container.
When you uninstall the Symantec Endpoint Encryption client software from an Active Directory computer, the **Active Directory Computers** container continues to list the inactive computer object.

If you reinstall the client software on that computer without changing the computer name, a new computer appears in the **Active Directory Computers** container. The original computer object is moved to the **Deleted Computers** container.

See “Deploying GPOs” on page 167.

## Deploying GPOs

To deploy a GPO, use the Group Policy Management Console snap-in in the Management Console. For instructions, refer to the Microsoft Management Console Help.

**Note:** If you use GPOs to distribute your MSIs, make sure that one GPO contains one MSI. Ensure that the Management Agent installs first. You can then install Drive Encryption or BitLocker Client, and Removable Media Encryption in any order.

If you install the BitLocker Client MSI on the client computer, then you cannot install the Drive Encryption MSI on the same client computer.

See “Forcing GPO updates” on page 167.

## Forcing GPO updates

GPO updates take approximately 90 minutes and no more than 120 minutes to be pushed to client computers. To manually accelerate deployment, you can force an immediate policy update.

**To force a GPO update**

1. On the client computer, click **Start**, and then **Run**.
2. Type `cmd` and press **Enter**.
3. At the command prompt, type:

   ```plaintext
gpupdate /force
   ```

   and press **Enter**.
4. At the confirmation message prompt to confirm a restart, type `Y` and press **Enter**.
See “Deploying GPOs” on page 167.

**About GPO priority sequence**

When you assign policies to a computer or a user object, consider the order in which they are applied. The order of application is:

1. Local
2. Site
3. Domain
4. Organizational Unit (OU)

Policies specific to a single computer or user object are local and are applied first. Policies are cumulative. The local group policy is at the bottom of the hierarchy and has the least significance. The policies that you assign after it, through the upper levels of the hierarchy, take precedence.

See “Deploying GPOs” on page 167.

See “About GPO assignment verification” on page 168.

**About GPO assignment verification**

The Group Policy Management Console (GPMC) snap-in includes a reporting capability. The Group Policy Report lets you verify that the GPOs that you assigned to client computers or users were processed as you intended. The report is also known as the Resultant Set of Policies (RSoP) report.

---

**Note:** The Group Policy Report shows only the results of GPO updates. The report does not show the installation settings, even if the MSIs are deployed as GPOs.

See “Verifying policy deployment in Active Directory” on page 243.

**Deploying native policies - process overview**

To deploy native policies, you must create managed computers groups then assign your policies to the appropriate groups. When the client computers check in, they receive their policies.
Table 8-2  Process for deploying native policies

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Create **Symantec Endpoint Encryption Managed Computers** groups | Create computer groups to which you assign your native policies.  
See “About Symantec Endpoint Encryption Managed Computers groups” on page 169.  
See “Creating Symantec Endpoint Encryption Managed Computers groups” on page 170. |
| Assign your native policy to a **Symantec Endpoint Encryption Managed Computers** group | To assign your native policy:  
See “Assigning native policies” on page 175. |
| Optionally, force a native policy update | Force a native policy update from a client computer:  
See “Forcing native policy updates” on page 176. |

**About Symantec Endpoint Encryption Managed Computers groups**

Native policies are assigned to individual computers, subgroups, or the groups that are located within the **Symantec Endpoint Encryption Managed Computers** container.

Before you can assign native policies to your managed computers, the computers need to be organized into groups. This task can be done from any Manager Computer. The group structure is saved in the Symantec Endpoint Encryption database and is available to all other Manager Computers.

The **Symantec Endpoint Encryption Managed Computers** container has two default groups: **SEE Unassigned** and **Deleted Computers**.

Computers in the **SEE Unassigned** group do not have policies assigned to them. These computers enforce their installation settings.

Computers are placed in the **SEE Unassigned** group if:

- Synchronization with a computer’s directory service is not enabled.
- The computer does not reside within the Active Directory forest or domain with which you synchronize.

Client computers appear in the **SEE Unassigned** group at the time that a computer checks in. However, if you manually delete a computer from the Active Directory...
domain, it does not appear in the SEE Unassigned group. It appears in the SEE Unassigned group at the time of the next synchronization.

When you uninstall the Symantec Endpoint Encryption client software from a computer, the Symantec Endpoint Encryption Managed Computers container continues to list the inactive computer.

When you delete a native client computer from the Symantec Endpoint Encryption Managed Computers container, the computer is moved to the Deleted Computers container.

Later, if you install the client software on that computer again without modifying its computer name, a duplicate computer entry appears in the Managed Computer Groups container. Refer to the Last Check-In Date column to identify the original, inactive computer and delete it.

To delete a native client computer from the Symantec Endpoint Encryption Managed Computers container, right-click the computer and select Delete.

To restore a deleted native client computer to its original managed computer group, click the Deleted Computers container, right-click the computer, and select Restore.

To move a native client computer to a different managed computer group, right-click the computer, select Change Group, and then navigate to and select the destination group.

See “Creating Symantec Endpoint Encryption Managed Computers groups” on page 170.

See “Moving computers from a Symantec Endpoint Encryption Managed Computers group to another group” on page 171.

See “Deleting a computer from a managed computer group” on page 172.

Creating Symantec Endpoint Encryption Managed Computers groups

To create a Symantec Endpoint Encryption Managed Computers group

1. In the Management Console, expand Symantec Endpoint Encryption Users and Computers.
2. Right-click Symantec Endpoint Encryption Managed Computers, and
4 Type the name of the new group.

The name must be unique within its group. For example, the Finance group can have two subgroups named Laptops and Desktops. The Human Resources group can also have two subgroups named Laptops and Desktops. However, two top-level groups that are listed within Symantec Endpoint Encryption Managed Computers cannot be named Human Resources.

5 Click OK.

See “Moving computers from a Symantec Endpoint Encryption Managed Computers group to another group” on page 171.

---

**Moving computers from a Symantec Endpoint Encryption Managed Computers group to another group**

To move a computer from a managed computer group to another group

1 In the Management Console, under Symantec Endpoint Encryption Managed Computers, navigate to the group that the computer currently belongs to and then select the computer that you want to move.

   Alternatively, while viewing a report in the Symantec Endpoint Encryption Reports snap-in, select the computer that you want to move.

   You can select more than one computer if needed.

2 In the right pane, right-click the computer and select Change Group.

   **Note:** In reports, this option is not available if you select a mix of native client computers and computers that belong to the same Active Directory as the Symantec Endpoint Encryption Management Server.

3 Navigate to and select the desired destination group.

4 Click OK.

See “Creating Symantec Endpoint Encryption Managed Computers groups” on page 170.
Deleting a computer from a managed computer group

To delete a client computer from a managed computer group

1 In the Management Console, under Symantec Endpoint Encryption Managed Computers, navigate to the group that the computer currently belongs to and then select the computer that you want to delete.

Alternatively, while viewing a report in the Symantec Endpoint Encryption Reports snap-in, select the computer that you want to delete from the group.

You can select more than one computer.

2 Right-click the selected computer and select Delete.

Note: In reports, this option is not available if you select a mix of native client computers and computers that belong to the same Active Directory as the Symantec Endpoint Encryption Management Server.

3 In the confirmation prompt, click Yes.

Note: Deleted native client computers are moved to the Deleted Computers node of the Symantec Endpoint Encryption Users and Computers snap-in.

Searching for specific computers

In the Symantec Endpoint Encryption Users and Computers snap-in, you can search for one or more client computers to view reports about them, or to view detailed configuration information about them.

To search for specific computers

1 In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Users and Computers snap-in.

2 Navigate to and select the Active Directory node in which you want to perform the search.

Alternatively, expand Symantec Endpoint Encryption Managed Computers, and select the managed computer group in which you want to perform the search.
In the **Enter Computer Names** box, type the host names of the computers whose details you want to view. Use carriage returns to separate the host names.

Alternatively, enter a partial computer name along with a wildcard search character.

4. Click **Run**.

See “About wildcard search characters” on page 173.

### About wildcard search characters

When you perform a search for client computers, you can enter a partial computer name in the **Enter Computer Names** box, along with a wildcard search character.

<table>
<thead>
<tr>
<th>Wildcard search character</th>
<th>Usage format</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>%PartialName%</td>
<td>Locates all of the client computers that include the partial name string in their name.</td>
<td>Typing %win% locates all of the computers that contain the string 'win' in their name.</td>
</tr>
<tr>
<td></td>
<td>OR</td>
<td>Alternately, type only % to search for all possible client computers in the selected domain, forest, tree, or group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>_ (underscore)</td>
<td>PartialName_</td>
<td>Locates all of the client computers that include the partial name string in their name, followed by one more character, such a number.</td>
<td>Typing Computer_ locates all of the computers that have names like Computer0, Computer2, ComputerA, and so on.</td>
</tr>
</tbody>
</table>
### Table 8-3  Wildcard search characters (continued)

<table>
<thead>
<tr>
<th>Wildcard search character</th>
<th>Usage format</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td>[CharacterSet]PartialName</td>
<td>Locates all of the client computers whose names begin with any of the specified characters and end with the partial name.</td>
<td>Typing [A-D]System or [ABCD]System locates all of the client computers whose names begin with the letters A, B, C, and D, and end with the word 'System'. For example, the search displays a list of computers with names such as ASystem, BSystem, CSystem, and DSystem.</td>
</tr>
<tr>
<td>[^]</td>
<td>PartialName[^CharacterSet]</td>
<td>Locates all of the client computers whose names begin with the partial name, and end with any character besides the specified ones. <strong>Note:</strong> The ^ symbol indicates a 'NOT' operator.</td>
<td>Typing System[^A-D] or System[^ABCD] locates all of the client computers whose names begin with 'System' and end with any character other than the characters A, B, C, and D. For example, the search displays a list of computers with names like SystemE, SystemF, SystemG, and so on.</td>
</tr>
</tbody>
</table>

See “Searching for specific computers” on page 172.
About assigning native policies

Native policies are applied at the computer level only; they cannot be assigned on a per user basis.

Native policies can be assigned to a group or a subgroup that is located within the Symantec Endpoint Encryption Managed Computers container.

Each policy is comprehensive and contains all of the possible configurable settings.

Only one policy can be applied to a computer at a time. If no policy is assigned to a computer, the computer reverts to its installation settings.

Native policies are applied when the client computer Management Agent checks in with the Management Server. However, if Drive Encryption or Symantec Endpoint Encryption for BitLocker is installed on the endpoint computer, users can perform an immediate check-in from the Management Agent console.

Clients in the Symantec Endpoint Encryption Managed Computers container cannot be assigned policies until they have checked in with the Management Server.

After a policy is successfully assigned, the Management Console displays the name of the policy now assigned to the group. The next time the client computers in this group check-in with the Management Server, they download this policy and apply it.

See “About Symantec Endpoint Encryption Managed Computers groups” on page 169.

See “Assigning native policies” on page 175.

See “Forcing native policy updates” on page 176.

Assigning native policies

To assign a native policy to a computer, subgroup, or group

1. From the Management Console, expand the Symantec Endpoint Encryption Users and Computers snap-in.
2. Select Symantec Endpoint Encryption Managed Computers.
3. Locate and right-click the recipient subgroup, or group of the policy.
4. Select Assign Policy to Group.
5 In the navigation dialog box, locate and select the native policy to be assigned to this group.

6 Click **OK** to dismiss the confirmation message.

7 Click **OK**.

See “About assigning native policies” on page 175.

### Forcing native policy updates

**To force a native policy update**

1 On the client computer, access the Management Agent console.

   If you do not have access to the client computer, ask the registered user or the client administrator to perform this step.

2 In the Check-in panel, click **Check-in**.

See “Assigning native policies” on page 175.

### About conflicting Symantec Endpoint Encryption policies

In Removable Media Encryption, when you configure both the Device and File Type Exclusions policy and the Access and Encryption policy, the Device and File Type Exclusions policy takes precedence. If a device is exempted from encryption, no other policies apply to it.

See “Configuring the Removable Media Encryption - Device and File Type Exclusions policy options” on page 139.

Using Autologon to bypass preboot authentication

This chapter includes the following topics:

■ About the Autologon Utility
■ Creating Autologon MSI files
■ Installing an Autologon MSI file on a client computer
■ Configuring the Drive Encryption - Autologon policy options

About the Autologon Utility

Use the Autologon Utility to configure Microsoft Windows client computers to bypass the preboot authentication screen that Symantec Endpoint Encryption Management Server enforces. By default, the Autologon function is not in effect for a computer. As an administrator, you can use Autologon when you want to update or deploy software on a client computer that requires multiple restarts. Patch management is an example of a process that can require multiple restarts.

Caution: A client computer running the Autologon utility is in a state of heightened vulnerability. Using Autologon inappropriately weakens the data protection that Drive Encryption provides. To minimize the associated risks, carefully review your procedures for enabling and disabling the Autologon function. The Autologon function should be disabled immediately when its intended use is achieved. For example, ensure that you disable the Autologon function immediately after you finish updating client computers.
To make the Autologon Utility available to client computers, generate Autologon client MSI files. You can create an MSI file in an enabled or disabled state. After you deploy and install the Autologon MSI on client computers, client administrators can use the Drive Encryption Administrator Command Line to manage Autologon. They can override the existing policy and enable or disable the Autologon functionality, as needed.

See “Creating Autologon MSI files” on page 178.

Creating Autologon MSI files

**Pre-requisite:** Make sure that you have installed the Autologon Utility and added it to the Management Console as a snap-in. For more information, see the "Adding the Autologon snap-in to the Management Console" topic in the Symantec Endpoint Encryption Installation Guide.

**To create Autologon client MSI files**

1. In the left pane of the Management Console, click Symantec Endpoint Encryption Autologon Utility.
2. On the Autologon Utility - Settings page, in the Management password field, type the management password that is currently in use.
3. Under Autologon, do one of the following:
   - To enable the Autologon feature and create the Autologon Infinite MSI file, click Always Autologon.
   - To disable the Autologon feature and create the Autologon NoAutologon MSI file, click Autologon only when activated by admin locally.
4. Under Autologon Precedence, do one of the following:
   - To enable users to log on to a locked out computer when Autologon is enabled, click Autologon takes precedence over client monitor lockout.
   - To prevent users from logging on to a locked out computer when Autologon is enabled, click Client monitor lockout takes precedence over Autologon.
5. Click Finish and save the MSI file.

**Note:** If you want to deploy, save the created MSI files in a folder that is in a shared network location. For example, the location can be in the domain controller's SYSVOL folder.

See “About the Autologon Utility” on page 177.
Installing an Autologon MSI file on a client computer

**Caution:** A client computer running Autologon is in a state of heightened vulnerability. To minimize the associated risks, carefully review your procedures for enabling and disabling Autologon. Autologon should be disabled immediately when its intended use is achieved.

**Note:** If you installed the Symantec Endpoint Encryption Client to a custom installation folder, make sure that you install the Autologon Utility in the same location.

To install an Autologon MSI file on a client computer

1. Navigate to the folder in which you saved the Autologon client MSI file that you created.
2. Double-click the MSI file that you want.
3. Restart the computer.
   - If the MSI file is Autologon NoAutologon, after the restart the user is prompted to authenticate during preboot.
   - If the MSI file is Autologon Infinite, after the restart the user is no longer prompted to authenticate during preboot

On a client computer, to enable, disable, or set the count of authentication bypasses, a client administrator can use the Drive Encryption Administrator Command Line. For more information, see the Symantec Endpoint Encryption Drive Encryption Administrator Command Line Guide.

See “About the Autologon Utility” on page 177.

See “Creating Autologon MSI files” on page 178.

Configuring the Drive Encryption - Autologon policy options

Creating and applying the Autologon policy

You can create and apply an Autologon GPO or native policy to enable or disable the Autologon Utility on a client computer. Also, you can use client administrator
credentials to manage the Autologon Utility locally using Administrator Command Line.

**Note:** To apply Autologon policy, you must first create the Autologon Utility MSI file, and then install the Autologon Utility on client computers.

Any recent update to the Autologon policy is applied to a client computer after the computer is restarted. Alternatively, the Autologon policy is also applied to client computers differently depending on whether the policy is a GPO or native policy.

A native policy is applied to a client computer when:

- The client computer user performs an immediate check-in from the Management Agent console.

- The communication interval time is met, and the client computer connects with the Symantec Endpoint Encryption Management Server automatically. (The communication interval time is the frequency with which the client computers attempt to connect with the Symantec Endpoint Encryption Management Server. The communication interval is set to 60 minutes by default.)

A GPO policy is applied to a client computer when:

- The client administrator forces policy update using the `gpupdate /force` command.

The following sequence shows the order of precedence in which the Autologon policy is applied to a managed client computer:

1. Autologon settings from a policy (highest precedence)
2. Autologon settings from Administrator Command Line
3. Autologon MSI (lowest precedence)

The Autologon Utility on a never-connected client computer can be managed only by Administrator Command Line. Therefore, you must select and deploy an Autologon policy before the client computer is disconnected from the managed network.

**Configuring Autologon for client monitor lockout scenario**

You can enforce a check-in policy to schedule and monitor your client computer through periodic contact with the server. When your client computer fails to contact the server within the prescribed schedule, the computer is locked out at preboot. The lockout, thereby, protects the data on your computer if the computer is lost or stolen.
However, if Autologon has been enabled when a computer is locked out, a user can log on to the computer without authenticating at preboot. To protect your data while Autologon is enabled, you can configure the Autologon precedence settings and enable the Client monitor lockout takes precedence over Autologon policy. After you enable this policy and when the lockout occurs, the computer remains in a preboot state after restart. Also, users cannot log on to the computer without the assistance from the help desk or until a client administrator unlocks the system.

To configure an Autologon policy

1. Access the Drive Encryption policy option using an install-time, Active Directory, or native policy.

2. On the Drive Encryption Computer Policy - Autologon page, do one of the following:

   ■ To disable the Autologon Utility on a client computer, click the Never Autologon policy option. Assign this policy to one or more client computers on which the Autologon Utility is already enabled. Applying this policy on a computer disables the Autologon Utility. When a user starts the client computer on which this policy is applied, the computer prompts for user authentication at preboot. The client computer boots into Windows only after successful user authentication.

   ■ To enable a client administrator to use the Administrator Command Line and manage the Autologon Utility, click the Autologon only when activated by admin locally policy option.

   ■ To enable the Autologon Utility on a client computer, click the Always Autologon policy option. Assign this policy to one or more client computers to enable the Autologon Utility. When a user starts a client computer on which this policy is applied, the client computer boots Windows without prompting for user authentication. This setting provides little protection to client computers. This option is selected by default.

   ■ To enable users to log on to a locked out computer when Autologon is enabled, click Autologon takes precedence over client monitor lockout.

   ■ To prevent users from logging on to a locked out computer when Autologon is enabled, click Client monitor lockout takes precedence over Autologon.

3. Click Next.
Note: If you upgraded to Symantec Endpoint Encryption version 11.0.0 or later, the Single Use and Recurring Autologon policy options appear disabled on the native and GPO Autologon policy pages. For more information, see the knowledge base article: Symantec Endpoint Encryption - Deprecated policy options

See “Accessing the Symantec Endpoint Encryption policy options” on page 111.
Using server-based commands

This chapter includes the following topics:

■ About server-based commands

■ Issuing server-based commands to encrypt or decrypt fixed disk drives - process overview

■ Issuing server-based commands to encrypt or decrypt fixed disk drives

■ Forcing a server-based command to execute on the client computers

■ Issuing server-based commands to cancel a pending command

■ Issuing the Change Web Access server command on client computers

About server-based commands

You can issue server-based commands from the Symantec Endpoint Encryption Users and Computers snap-in in the Symantec Endpoint Encryption Management Console, and from reports in the Symantec Endpoint Encryption Reports snap-in. The commands are to encrypt or decrypt fixed disk drives on the computers that:

■ Have Microsoft Windows installed

■ Have Opal v2 compliant drives

■ Have a version of Symantec Endpoint Encryption Full Disk 8.2.1 or later installed

Note: If a computer has managed drives and unmanaged drives, the command is applied to the managed as well as unmanaged drives.
**Note:** If a computer has a Remote Decryption policy enabled, you cannot encrypt the drives. The encrypt command fails silently.

Server-based commands can be applied to groups of computers, individual computers, or one or more drives on a single computer. If a group does not contain computers—such as groups that contain only users—you receive an error and the command is not issued. The server-based command menu is not available for the Deleted Computers group.

**Note:** The server-based commands are not applicable to the Mac FileVault Client computers group.

Once a client computer checks in with Symantec Endpoint Encryption Management Server, it receives the server-based command. The Management Server tries to send the command for up to 30 days. After 30 days, the command expires and is deleted. Commands not yet received by computers can be canceled.

The Symantec Endpoint Encryption Server Command snap-in provides reports on issued commands. It also provides an interface for canceling pending commands.

To issue or cancel a server command from the **Symantec Endpoint Encryption Users and Computers** snap-in, you must have either the Server Administrator role, or the Policy Administrator role.

To issue or cancel a server command from a report in the **Symantec Endpoint Encryption Reports** snap-in, you must have the Server Administrator role, or the Policy Administrator role and the Report Administrator role.

To cancel a server command from the **Symantec Endpoint Encryption Server Commands** snap-in, you must have either the Server Administrator role or the Policy Administrator role.

**Note:** On a client computer, a client administrator can locally reverse a server-based command. The reversal can be done by running the appropriate commands from the Drive Encryption Administrator Command Line interface. See **Symantec Endpoint Encryption Drive Encryption Administrator Command Line Guide**.
# Issuing server-based commands to encrypt or decrypt fixed disk drives - process overview

## Table 10-1

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt or decrypt all drives on all of the computers within an Active Directory or Symantec Endpoint Encryption Managed Computers group</td>
<td>To encrypt or decrypt all drives on all of the computers within an Active Directory or Symantec Endpoint Encryption Managed Computers group: See “To encrypt or decrypt all drives on all of the computers within an Active Directory or Symantec Endpoint Encryption Managed Computers group” on page 186.</td>
</tr>
<tr>
<td>Encrypt or decrypt all fixed disk drives on a computer</td>
<td>To encrypt or decrypt all fixed disk drives on a computer: See “To encrypt or decrypt all fixed disk drives on a computer” on page 187.</td>
</tr>
<tr>
<td>Encrypt or decrypt one or more fixed disk drives on a computer</td>
<td>To encrypt or decrypt one or more fixed disk drives on a computer: See “To encrypt or decrypt one or more fixed disk drives on a computer” on page 187.</td>
</tr>
<tr>
<td>Force a command to execute</td>
<td>To force a command to execute: See “Forcing a server-based command to execute on the client computers” on page 188.</td>
</tr>
<tr>
<td>Cancel a pending encryption or decryption command for all computers</td>
<td>To cancel a pending encryption or decryption command for all computers: See “To cancel a pending encryption or decryption command for all computers” on page 189.</td>
</tr>
<tr>
<td>Cancel a pending encryption or decryption command for one computer</td>
<td>To cancel a pending encryption or decryption command for one computer: See “To cancel a pending encryption or decryption command for one computer” on page 190.</td>
</tr>
</tbody>
</table>
Issuing server-based commands to encrypt or decrypt fixed disk drives

When you want to upgrade your client computers with a new release of an operating system (for example, from Windows 8 to Windows 8.1), ensure that you decrypt the encrypted disk of your client computers before you upgrade. Decrypting the encrypted disk prevents any data loss or damage to your disks. For more information on upgrading the operating system on the client computers, see Symantec Endpoint Encryption Client Online Help.

To issue a server command from the Symantec Endpoint Encryption Users and Computers snap-in, you must have either the Server Administrator role, or the Policy Administrator role.

To issue a server command from a report in the Symantec Endpoint Encryption Reports snap-in, you must have either the Server Administrator role, or both the Policy Administrator role and the Report Administrator role.

**Note:** When you upgrade Symantec Endpoint Encryption Management Server versions earlier than 11.0.0, and the early versions have the Novell eDirectory services enabled, you can view the Novell eDirectory Computers option in the Symantec Endpoint Encryption Users and Computers snap-in. In such cases, you can execute the server-based encrypt and decrypt commands to Novell clients through the upgraded server, Symantec Endpoint Encryption Management Server 11.x.

To encrypt or decrypt all drives on all of the computers within an Active Directory or Symantec Endpoint Encryption Managed Computers group

1. Open the Management Console.
2. Expand the Symantec Endpoint Encryption Users and Computers snap-in.
3. Navigate to the group or subgroup you want to receive the command.
4. Right-click the group or subgroup and select Set Server Commands. Alternatively, select the group or subgroup and click Actions > Set Server Commands.
5. Do one of the following:
   - To encrypt all drives on the selected group or subgroup, click Encrypt All Drives.
To decrypt all drives on the selected group or subgroup, click Decrypt All Drives.

6 In the Symantec Endpoint Encryption Manager message box:
   ■ To apply the command to the selected group as well as to all the subgroups within it, check Apply command to sub groups.
   ■ To confirm issuing the command, click Yes.

To encrypt or decrypt all fixed disk drives on a computer
1 Open the Management Console.
2 Expand the Symantec Endpoint Encryption Users and Computers snap-in, and navigate to the computer on which you want to encrypt or decrypt all of the fixed disk drives.
   Alternatively, while viewing a report in the Symantec Endpoint Encryption Reports snap-in, select the computer on which you want to encrypt or decrypt all of the fixed drives.
3 In the right pane, right-click the computer, and select Set Server Commands.
   Alternatively, select the group or subgroup and click Actions > Set Server Commands.
4 Do one of the following:
   ■ To encrypt all fixed disk drives on the selected computer, click Encrypt All Drives.
   ■ To decrypt all fixed disk drives on the selected computer, click Decrypt All Drives.
5 To confirm issuing the command in the Symantec Endpoint Encryption Manager message box, click Yes.

To encrypt or decrypt one or more fixed disk drives on a computer
1 Open the Management Console.
2 Expand the Symantec Endpoint Encryption Users and Computers snap-in and navigate to the computer on which you want to encrypt or decrypt one or more fixed-disk drives.
   Alternatively, while viewing a report in the Symantec Endpoint Encryption Reports snap-in, select the computer on which you want to encrypt or decrypt one or more fixed-disk drives.
3 In the right pane, double-click the computer or right-click the computer and click Show Details.
4 In the Computer Properties window, click the Fixed Drives tab.
5 Locate the physical disk that contains the drive(s) that you want to encrypt or decrypt. Right-click the disk and select Set Server Commands. Do one of the following:

- To encrypt all of the logical drives on the physical disk, click Encrypt Drive.
- To decrypt all of the logical drives on the physical disk, click Decrypt Drive.

6 To confirm issuing the command in the Symantec Endpoint Encryption Manager message box, click Yes.

Forcing a server-based command to execute on the client computers

For the server-based commands to execute on the client computers, the client user must establish communication with Symantec Endpoint Encryption Management Server. You can recommend that the users establish communication with the server.

To force a server-based command to execute, a user must

1 Open the Symantec Endpoint Encryption Management Agent.
2 On the Internal Drives tab, click Status.
3 Click Check-in.

Issuing server-based commands to cancel a pending command

When you issue a server-based command, it resides in a database for up to 30 days, until a target client computer checks in with Symantec Endpoint Encryption Management Server and receives the command. At that point, the command status for that computer changes from Pending to Sent to Endpoint. As long as a computer’s command status is Pending, the command for that computer can be canceled. When a command is issued for multiple computers, it is possible to have a mix of statuses associated with that command, as computers check in at various intervals.

You can cancel a command in one of the following ways:

- Cancel a command for all computers—If you issued a command that applied to multiple computers, you can cancel it for all of the computers. Computers that have not checked in yet do not receive or process the command.
Cancel a command for one computer—You can cancel commands for each computer.

**Note:** To cancel a pending server command from the Symantec Endpoint Encryption Server Commands snap-in, you must have either the Server Administrator role, or the Policy Administrator role.

**To cancel a pending encryption or decryption command for all computers**

1. Open the Management Console.
2. In the left pane, expand Symantec Endpoint Encryption Server Commands.
3. Navigate to the command you want to cancel.
4. To preview the computers that are listed when the command is canceled, double-click the command or right-click and select **Show Details**.

   The **Command Assignment** window lists the computers and their command status. The cancellation command applies to all computers with the command status still showing as **Pending**.

   **Note:** The computers whose command status is **Sent to endpoint** are unaffected by the cancellation.

5. Click **Close**.
6. In the **Command Assignment** window, the command is still selected. Right-click the command and click **Delete**.
7. To proceed with the deletion of the command in the Symantec Endpoint Encryption Manager message box, click **Yes**.
8. To verify the cancellation:
   - Double-click the command or select **Show Details**.
     The **Command Assignment** window now displays the computers to which the command had already been sent and the computers that are marked for delete.
   - In the left pane, expand Symantec Endpoint Encryption Reports. Click **Admin Log**. A message is logged for the cancellation of the encryption or decryption command. The message also consists of:
     - Date or timestamp
     - Identification of your Windows domain\user name
To cancel a pending encryption or decryption command for one computer

1. Open the Management Console.
2. In the left pane, expand the Symantec Endpoint Encryption Users and Computers snap-in and navigate to the computer for which you want to cancel a pending command.
   Alternatively, while viewing a report in the Symantec Endpoint Encryption Reports snap-in, select the computer for which you want to cancel a pending command.
3. In the right pane, double-click the computer or right-click it and select Show Details.
4. In the Computer Properties window, click the Server Commands tab.
5. Right-click the pending command you want to cancel and click Delete.

---

**Note:** To cancel a pending server command from the Symantec Endpoint Encryption Users and Computers snap-in, you must have either the Server Administrator role, or the Policy Administrator role.

To cancel a pending a server command from a report in the Symantec Endpoint Encryption Reports snap-in, you must have either the Server Administrator role, or the Policy Administrator role.

---

6. To proceed with the deletion of the command in the Symantec Endpoint Encryption Manager message box, click Yes.
7. To verify the cancellation:
   - The computers that are marked for delete appear with status as 'Deleted' on the Server Commands tab.
   - In the left pane, expand Symantec Endpoint Encryption Reports. Click Admin Log. A message is logged for the removal of the encryption or decryption command. The message also consists of:
     - Date or timestamp
     - Identification of your Windows domain\user name
     - The Management Console computer name from which the command was issued
Activity description

The name of the target computer for which the command is issued.

If the target computer is joined to a domain or is a part of an Active Directory, the name of the domain or the Active Directory tree appears. If the target computer is local, the domain is displayed as <local>.

Issuing the Change Web Access server command on client computers

Use the Change Web Access server command to create and distribute the new Internet Information Services (IIS) client/server communication credentials and server parameters to your client computers. You do not need to create or deploy a modified Management Agent MSI.

Note: The Change Web Access command is supported starting from Symantec Endpoint Encryption 11.1.0 only. The Change Web Access command is not applicable on the Mac FileVault Client computers.

You can use the Change Web Access server command to:

- Change the Windows user credentials used in the IIS basic authentication
- Redirect your client computers to access a different web server that uses the current database

You can issue the Change Web Access server command with the following new parameters:

- Windows authentication credentials for IIS
- Web server name
- Port number
- Protocol type
- SSL certificate

To issue a server command from the Symantec Endpoint Encryption Users and Computers snap-in, you must have either the Server Administrator role or the Policy Administrator role.
Note: Ensure to issue the Change Web Access command before the password of the current user used for IIS authentication expires. Change Web Access command does not let you change the password of an existing user used for IIS authentication. If the password of the existing user is about to expire in near future, you must provide a different IIS access user account in Active Directory and specify that user account while issuing the Change Web Access command.

To create the Change Web Access server command for the client computers

Note: Before you complete this procedure ensure that you select the check boxes corresponding to the parameters that you want to apply on the client computers.

1. Open the Management Console.
2. Expand the Symantec Endpoint Encryption Users and Computers snap-in.
3. Navigate to the group or subgroup to which you want to apply the command.
4. Right-click the group or subgroup and point to Set Server Commands, and click Change Web Access to open the Change Web Access Command Parameters dialog box.
5. To set new access credentials for your web server that uses the current database, under Web server, select Include web server details.
6. From the Host list box, select the web server for which you want to change access credentials.
7. In the URL box, type the Symantec Endpoint Encryption communication service website for the Symantec Endpoint Encryption Management Server.
8. To use an SSL certificate to connect with a web service, under Certificate data, select Include certificate. The current certificate details appear in the Type and Hash text boxes that cannot be edited.

Note: The Include certificate option is disabled if you have not configured your web server for HTTPS communication. To enable SSL/HTTPS communication in IIS, you must first obtain a certificate that is used to encrypt and decrypt information over your network.
To change the Windows user credentials used for the IIS basic authentication, under **Authentication parameters**, select **Include user name** and **Include password**, and then enter the new user name and password in the text boxes respectively. The current Windows user domain name appears in the **Include domain name** text box that cannot be edited.

To deploy the web access server command, click **OK**.
Using server-based commands

Issuing the Change Web Access server command on client computers
Viewing Symantec Endpoint Encryption reports

This chapter includes the following topics:

- About reports in Symantec Endpoint Encryption
- Customizing the appearance of reports
- Viewing reports in the Management Console
- Creating and editing custom reports

About reports in Symantec Endpoint Encryption

You can use the reporting functionality of the Management Console to obtain and view information about:

- Client computers in Active Directory
- Native client computers in a different domain from Symantec Endpoint Encryption Management Server
- Policy settings that affect computers and users in Active Directory
- Native policy settings that affect computers and users in a different domain from Symantec Endpoint Encryption Management Server
- Directory service synchronization of the client computers in Active Directory or Novell eDirectory
- Server Commands that have been issued to the client computers that have Drive Encryption installed.
- Failed login attempts that involve the Management Password
Changes to administrative server roles

You need permissions to access the reports functionality.

See “Permissions required to access reports” on page 196.

Permissions required to access reports

The following roles and permissions are required for reports functionality:

- Symantec Endpoint Encryption Reports snap-in: requires the Server Administrator role or the Report Administrator role.
- Symantec Endpoint Encryption Users and Computers snap-in: requires the Server Administrator role or the Policy Administrator role.
- Symantec Endpoint Encryption Commands snap-in: requires the Server Administrator role or the Policy Administrator role.
- Symantec Endpoint Encryption Custom reports: requires the Server Administrator role or Reports role. Access to custom reports also requires that the user have administrative rights on the Symantec Endpoint Encryption Management Server.

Types of reports

Symantec Endpoint Encryption provides two types of reports:

- Tabular reports
- Pie graphs

In the tabular reports, raw data is displayed in the right-hand pane of the Management Console. You can also right-click individual computer records in a report and select Show Details to view more details about those computers. This functionality is available only in the reports that display information about individual computers, such as the Computer Status Report.

In addition, all of the tabular reports let you customize the columns that are displayed. All of the reports let you hide the columns that you do not want to see. A few reports let you extend the columns that are displayed beyond the default set.

See “Changing the columns that are displayed in a report” on page 198.

In pie graph reports, each slice indicates a percentage value of the measured metric or parameter. These reports also display raw numerical values beneath the graphical representation.
Additional features in reports

All of the reports in the Symantec Endpoint Encryption include the following features:

■ You can print the information that is displayed in reports. You can also preview the printout to make sure that your printer is configured correctly.

■ In tabular reports, you can click Export to save the displayed information as a .csv file or a .pdf file. They also include a pagination function that you can use to navigate multiple pages of reported data.

■ (Applies to client computers running 8.2.1 or earlier versions of the software) You can click Recover in tabular reports to export a .dat recovery file from the selected client computer. You can use the .dat file to recover data if that computer fails to boot.

■ You can double-click the client computers that are listed in reports to view more detailed policy and encryption status information.

■ You can right-click client computers in reports to perform functions such as issuing server commands and moving them to a different managed computer group.

Note: Server commands are available only in the reports that display information about Drive Encryption. In addition, you must have either the Sever Administrator role or the Policy Administrator role to issue server commands.

See “Issuing server-based commands to encrypt or decrypt fixed disk drives” on page 186.
See “Moving computers from a Symantec Endpoint Encryption Managed Computers group to another group” on page 171.
See “Deleting a computer from a managed computer group” on page 172.

In addition to these standard features, you can perform searches for specific client computers in the reports that are available in the Symantec Endpoint Encryption Users and Computers snap-in.

See “Searching for specific computers” on page 172.

Customizing the appearance of reports

This section contains the following topics:

■ Changing the columns that are displayed in a report
Changing the columns that are displayed in a report

You can customize reports to display more columns or fewer columns, depending on your information needs.

You can extend the following reports to display an extended number of columns:

- Computer Status Report
- Computers not Encrypting to Removable Media Encryption
- Computers with Decrypted Drives
- Computers with Expired Certificates
- Computers with Specified Users
- Computers without Drive Encryption installed
- Computers without Removable Media Encryption installed
- Non-Reporting computers
- Computers with Hardware Encrypted Drives
- Removable Media Encryption Details Report
- Mac Computers FileVault Status

See “About the extended columns in reports” on page 199.

**Note:** You can change the columns that are displayed in one report at a time. Repeat the following procedure for each report that you want to customize.

**To change the columns that are displayed in a report**

1. In the navigation pane of the Management Console, expand Symantec Endpoint Encryption Reports.
2. Right-click the report that you want to customize, and select Configure Columns Displayed.
3. In the Select Columns dialog box, check the columns that you want to add to the report, or uncheck the columns that you want to hide.
   
   Alternatively, to undo any previous changes that you made, click Defaults to restore the default columns for the report.
About the extended columns in reports

Some reports in Symantec Endpoint Encryption let you extend the columns that are displayed beyond the default set of columns. This topic describes all of the extended columns that are available in the Symantec Endpoint Encryption Reports snap-in.

Note: Some of these columns might appear as default columns in a few reports.

See “Changing the columns that are displayed in a report” on page 198.

Table 11-1 The extended columns that you can add to reports

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Tag</td>
<td>The System Management BIOS (SMBIOS) asset tag of the client computer. If the data does not exist on the client computer, this column displays <em>Not available</em> as its value.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the <em>Symantec Endpoint Encryption Users and Computers</em> snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>MA Version</td>
<td>The version number of the Management Agent client that is currently installed on the client computer.</td>
</tr>
<tr>
<td>MA Build Number</td>
<td>The build number of the Management Agent client that is currently installed on the client computer.</td>
</tr>
<tr>
<td>MA Installation Date</td>
<td>The date and time that the Management Agent client was installed on the client computer.</td>
</tr>
<tr>
<td>Operating System</td>
<td>The name of the operating system that is currently installed on the client computer.</td>
</tr>
<tr>
<td>Column name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Part Number</td>
<td>The System Management BIOS (SMBIOS) part number of the client computer. If</td>
</tr>
<tr>
<td></td>
<td>the data does not exist on the client computer, this column displays Not</td>
</tr>
<tr>
<td></td>
<td>available as its value.</td>
</tr>
<tr>
<td>CA Certificate Expiration Date</td>
<td>The expiration date and time of the Certificate Authority (CA) certificate</td>
</tr>
<tr>
<td></td>
<td>that is stored on the client computer. If the data does not exist on the</td>
</tr>
<tr>
<td></td>
<td>client computer, this column displays Not available as its value.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The System Management BIOS (SMBIOS) serial number of the client computer.</td>
</tr>
<tr>
<td></td>
<td>If the data does not exist on the client computer, this column displays Not</td>
</tr>
<tr>
<td></td>
<td>available as its value.</td>
</tr>
<tr>
<td>System Type</td>
<td>Indicates whether the client computer has a 32-bit or 64-bit operating</td>
</tr>
<tr>
<td></td>
<td>system installed.</td>
</tr>
<tr>
<td>Computer Model</td>
<td>Indicates the model of the Macintosh client computer.</td>
</tr>
</tbody>
</table>
Table 11-1 The extended columns that you can add to reports *(continued)*

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileVault Status</td>
<td>Indicates the current state of the FileVault application. The following values are possible:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Off</strong> - FileVault is not currently managed by Symantec Endpoint Encryption for FileVault.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Off - Managed</strong> - FileVault is currently managed by Symantec Endpoint Encryption for FileVault, but has been disabled by the user.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>On - Managed (with IRK)</strong> - FileVault is active, the Personal Recovery Key (PRK) is not stored in the Symantec Endpoint Encryption Management Server database, and the Institutional Recovery Key (IRK) policy setting is enabled.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>On - Managed (with PRK)</strong> - FileVault is active, the Personal Recovery Key (PRK) is stored in the Symantec Endpoint Encryption Management Server database, and the Institutional Recovery Key (IRK) policy setting is disabled.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>On - Managed (with PRK and IRK)</strong> - FileVault is active, the Personal Recovery Key (PRK) is stored in the Symantec Endpoint Encryption Management Server database, and the Institutional Recovery Key (IRK) policy setting is enabled.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Unknown</strong> - The FileVault encryption status is unknown, or the Symantec Endpoint Encryption for FileVault has not transmitted the information to the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Drive Encryption columns</td>
<td></td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
</tbody>
</table>
### Table 11-1 The extended columns that you can add to reports (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE Version</td>
<td>The version number of Drive Encryption that is currently installed on the client computer.</td>
</tr>
<tr>
<td>DE Build Number</td>
<td>The build number of Drive Encryption that is currently installed on the client computer.</td>
</tr>
<tr>
<td>DE Installation Date</td>
<td>The date and time that Drive Encryption was installed on the client computer.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Number of Drives</td>
<td>The number of physical drives on the client computer.</td>
</tr>
<tr>
<td>Hardware Encrypted Drives</td>
<td>Indicates whether the client computer has hardware encrypted drives or not.</td>
</tr>
</tbody>
</table>

#### BitLocker Encryption columns

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BE Version</td>
<td>The version number of Symantec Endpoint Encryption for BitLocker that is currently installed on the client computer.</td>
</tr>
<tr>
<td>BE Build Number</td>
<td>The build number of Symantec Endpoint Encryption for BitLocker that is currently installed on the client computer.</td>
</tr>
<tr>
<td>BE Installation Date</td>
<td>The date and time when Symantec Endpoint Encryption for BitLocker was installed on the client computer.</td>
</tr>
</tbody>
</table>

#### Removable Media Encryption columns


<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removable Media Access Utility</td>
<td>Indicates whether the Removable Media Access Utility is copied to removable media devices. This column also specifies whether the Windows version, the Mac OS X version, or both versions of the Removable Media Access Utility are copied.</td>
</tr>
<tr>
<td>RME AutoRun Enabled</td>
<td>(Applies to client computers running 8.2.1 or earlier versions of the software) Indicates whether the AutoRun functionality is enabled for the Removable Media Access Utility.</td>
</tr>
<tr>
<td>RME Build Number</td>
<td>The build number of Removable Media Encryption that is currently installed on the client computer.</td>
</tr>
<tr>
<td>RME Default Password Aging</td>
<td>Indicates whether a password aging policy is in effect for Default Passwords.</td>
</tr>
<tr>
<td>RME Device Access Control</td>
<td>Indicates the level of read or write access on the removable media devices that are connected to the client computer.</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
<tr>
<td>RME Device Memo</td>
<td>The optional memo text that an administrator saved.</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Format</td>
<td>Indicates whether files on removable media devices are encrypted using the SEE RME format for Symantec Endpoint Encryption versions 11.0 and later, or the SEE RS format for Symantec Endpoint Encryption version 8.2.1. For the client computers that use a version of Removable Media Encryption earlier than 11.0.0 MP2, no value is displayed.</td>
</tr>
</tbody>
</table>
### Table 11-1  The extended columns that you can add to reports *(continued)*

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RME Exempted Product ID</td>
<td>The product ID (PID) of the removable media device that is exempted from encryption.</td>
</tr>
<tr>
<td>RME Exempted Vendor ID</td>
<td>The vendor ID (VID) of the removable media device that is exempted from encryption.</td>
</tr>
<tr>
<td>RME Exempted File Types</td>
<td>Indicates the multimedia file groups, such as audio, image, and video files, that are exempted from encryption on removable media devices. Alternatively, this column indicates whether no file groups are exempted from encryption.</td>
</tr>
<tr>
<td>RME File Type Exemptions</td>
<td>The file extensions that are exempted from automatic encryption on the removable media devices that are connected to the client computer.</td>
</tr>
<tr>
<td>RME Installation Version</td>
<td>The version number of Removable Media Encryption that was originally installed on the client computer.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Passwords</td>
<td>Indicates the type of password that users are allowed to set. Depending on the current policy in force, one or more of the following values might be displayed in this column (multiple values are separated by semicolons):</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Default</strong> – Users are allowed to set a Default Password.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Session Default</strong> – Users are allowed to set Session Passwords.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>None</strong> – (Applies to client computers running 8.2.1 or earlier versions of the software) Users are not allowed to set a Default password, or a Session password, or a Device Session Default Password.</td>
</tr>
<tr>
<td>RME Recovery Certificate</td>
<td>The serial number of the recovery certificate that is in effect on the client computer. If there is no recovery certificate, this column displays <strong>Not Enabled</strong> as the value.</td>
</tr>
</tbody>
</table>
**Table 11-1** The extended columns that you can add to reports *(continued)*

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RME Self-Decrypting Archives</td>
<td>Indicates whether users can create self-decrypting archives on the computers that have Removable Media Encryption installed.</td>
</tr>
<tr>
<td>RME Session Default Password Aging</td>
<td>Indicates whether a password aging policy is in effect for Session Passwords.</td>
</tr>
<tr>
<td>RME SHA Type</td>
<td>The SHA type that is used in the encryption algorithm. This column displays a value only for the computers that have an earlier version of Symantec Endpoint Encryption Removable Storage installed.</td>
</tr>
<tr>
<td>RME User Choice Default Policy</td>
<td>Indicates the default action that is specified for the <code>Allow users to choose</code> option of the Automatic Encryption policy setting. Alternatively, indicates when user choice is not enabled.</td>
</tr>
<tr>
<td>RME Version</td>
<td>The version number of Removable Media Encryption that is currently installed on the client computer.</td>
</tr>
<tr>
<td>RME Workgroup Key</td>
<td>Indicates whether a group key is in use on the client computer.</td>
</tr>
<tr>
<td>RME VDI Catalog ID</td>
<td>The ID of the XenDesktop machine catalog that the VDI client belongs to.</td>
</tr>
<tr>
<td>RME VDI Catalog Name</td>
<td>The name of the XenDesktop machine catalog that the VDI client belongs to.</td>
</tr>
<tr>
<td>RME VDI Client</td>
<td>Indicates whether the client computer is a XenDesktop VDI client.</td>
</tr>
<tr>
<td>RME VDI Client Image</td>
<td>Indicates whether the VDI client image is a Master image or a Client image.</td>
</tr>
<tr>
<td>RME VDI Client Image Pool</td>
<td>Indicates whether the client image belongs to a predefined Static pool, or to a Random pool. This column does not display a value if the VDI client image is a Master image.</td>
</tr>
</tbody>
</table>
Viewing reports in the Management Console

This section includes the following topics:

- Viewing information about specific computers in Active Directory
- Viewing the encryption status of computers that have either Drive Encryption or Removable Media Encryption installed
- Viewing the synchronization status of forests in Active Directory
- Viewing the history of actions performed in the Management Console
- Viewing the history of logged events on client computers
- Viewing a list of computers that currently do not encrypt files on removable media devices
- Viewing a list of computers whose fixed drives are currently not encrypted
- Viewing a list of computers whose certificates expire within a specified number of days
- Viewing a list of computers on which a specified user is registered
- Viewing a list of computers that do not have Drive Encryption installed
- Viewing a list of computers that do not have Removable Media Encryption installed
- Viewing a list of removable media devices that are exempted from encryption
- Viewing a list of computers that have not checked in within a specified number of days
- Viewing the synchronization status of your Novell eDirectory
- Viewing information about computers that have Opal v2 compliant drives
- Viewing the percentage of computers that have fully or partly encrypted drives
- Viewing the policy details of computers that have Removable Media Encryption installed
- Viewing the encryption status of Macintosh computers that have Symantec Endpoint Encryption for FileVault installed
- Viewing the encryption status of computers that have Symantec Endpoint Encryption for BitLocker installed
- Viewing the history of server commands
- Verifying policy deployment in Active Directory
Viewing the synchronization status of forests in Active Directory

The Active Directory Forests Synchronization Status report displays information about the most recent synchronization of Active Directory.

**Table 11-2**

Default columns that are displayed in the Active Directory Forests Synchronization Status report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forest Name</td>
<td>The name of the Active Directory forest that was synchronized.</td>
</tr>
<tr>
<td>Administrator Name</td>
<td>The administrator user name in Active Directory that was used to log on to the directory service server of the forest that was synchronized.</td>
</tr>
<tr>
<td>administrator Domain</td>
<td>The Active Directory domain of the administrator account that was used to authorize the synchronization.</td>
</tr>
<tr>
<td>Last Synchronization</td>
<td>The date and time of the most recent successful synchronization.</td>
</tr>
<tr>
<td>Total Computers</td>
<td>The number of computers that were synchronized. This number includes even the computers that are not managed by Symantec Endpoint Encryption.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

**To view the synchronization status of forests in Active Directory**

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Active Directory Forests Synchronization Status report.

Viewing the history of actions performed in the Management Console

The Admin Log report provides a detailed log of all policy administrator activities. These activities include failed logins that involved the Management Password, and changes to the assignment of administrative server roles. Failed logins can occur when an administrator tries to access a snap-in without the proper password. They can also occur when an administrator tries to install or upgrade the Management Console.
# Table 11-3: Default columns that are displayed in the Admin Log report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date-Time</td>
<td>The date and time on which the administrator activity occurred.</td>
</tr>
<tr>
<td>User</td>
<td>The Active Directory domain and user name of the policy administrator who initiated the activity.</td>
</tr>
<tr>
<td>Management Computer</td>
<td>The host name of the management computer that was used to initiate the activity.</td>
</tr>
<tr>
<td>Activity Description</td>
<td>A brief description of the activity that the policy administrator initiated.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

## To view the history of actions performed in the Management Console

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Admin Log report.
3. (Optional) To specify a start date for reporting data, check Activity From.
   If you do not check Activity From, the report filters the earliest available data by using the remaining query conditions.
4. (Optional) To specify an end date for reporting data, check To.
   If you do not check To, the current date is selected as the end date in the report.
5. (Optional) In the User box, type the name of the administrator whose policy changes you want to view.
   Alternatively, to view all of policy changes, regardless of the administrator who made them, type the % character.
6. (Optional) In the Computer box, type the name of the management computer that was used to make the policy changes that you want to view.
   Alternatively, to view the policy changes that were made using an unspecified management computer, type the % character.
7. Click Run.
Note: If you click Run without supplying any query conditions, the report gathers and displays all of the available historical data about policy changes.

Viewing the history of logged events on client computers

The Client Events Log report displays a list of logged events on client computers.

Table 11-4 Default columns that are displayed in the Client Events Log report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date-Time</td>
<td>The date and time on which the logged event occurred.</td>
</tr>
<tr>
<td>User</td>
<td>Active Directory domain and user name of the user who was logged on to the client computer when the event occurred.</td>
</tr>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer on which the event occurred.</td>
</tr>
<tr>
<td>Event Description</td>
<td>A brief description of the logged event.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

Note: Client computers that boot in UEFI mode do not log unsuccessful logon attempts at the preboot authentication screen. Administrators can use the Client Event Log report to view the number of unsuccessful preboot authentication attempts only for client computers that boot in BIOS mode.

See “Changing the columns that are displayed in a report” on page 198.

To view the history of logged events on client computers

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Client Events Log report.
3. (Optional) To specify a start date for reporting data, check Events From.
   If you do not check Events From, the report filters the earliest available data by using the remaining query conditions.
4. (Optional) To specify an end date for reporting data, check To.
   If you do not check To, the current date is selected as the end date in the report.
5  (Optional) In the **User** box, type the name of the registered user whose logged actions you want to view.

Alternatively, to view all of the logged events, regardless of the user who was logged in when the events occurred, type the % character.

6  (Optional) In the **Computer** box, type the host name of the client computer whose event logs you want to view.

Alternatively, to view the events that were logged on all of the client computers on the network, type the % character.

7  Click **Run**.

**Note:** If you click **Run** without supplying any query conditions, the report displays all available event logs from all client computers on the network.

---

### Viewing information about specific computers in Active Directory

The Computer Status Report displays information about specific computers in Active Directory. Use this report to verify deployment after you finish installing the Drive Encryption functionality on computers in Active Directory.

When a Microsoft Windows client computer checks in, it sends data for the online method of the Help Desk Recovery authentication process. If you detect the client computers that have not checked in, you can troubleshoot by using other tools. For example, you can use the Group Policy Report or the Windows system event logs to troubleshoot.

The computer sends data for the /B, /O, and /S options of the Recover Program. If a Microsoft Windows client computer fails to boot, you might have to export the computer-specific recovery data that is required for a Recover /B or Recover /O operation. This functionality is available only for Symantec Endpoint Encryption Full Disk 8.2.1, or an earlier compatible version.

<table>
<thead>
<tr>
<th>Table 11-5</th>
<th>Default columns that are displayed in the Computer Status Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
</tbody>
</table>
Table 11-5: Default columns that are displayed in the Computer Status Report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Device Access Control</td>
<td>Indicates the level of read or write access on the removable media devices that are connected to the client computer.</td>
</tr>
<tr>
<td>RME Encryption Format</td>
<td>Indicates whether files on removable media devices are encrypted using the SEE RME format for Symantec Endpoint Encryption versions 11.0 and later, or the SEE RS format for Symantec Endpoint Encryption version 8.2.1. For the client computers that use a version of Removable Media Encryption earlier than 11.0.0 MP2, no value is displayed.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
</tbody>
</table>
### Table 11-5

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removable Media Access Utility</td>
<td>Indicates whether the Removable Media Access Utility is copied to removable media devices. This column also specifies whether the Windows version, the Mac OS X version, or both versions of the Removable Media Access Utility are copied.</td>
</tr>
<tr>
<td>RME Self-Decrpyting Archives</td>
<td>Indicates whether users can create Self-Decrpyting Archive files on the computers that have Removable Media Encryption installed.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

**To view information about specific computers in Active Directory**

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click **Computer Status Report**.
3. In the **Enter Computer Names** box, type the host names of the computers whose details you want to view.
   
   To view information about all of the computers in Active Directory, type %. Alternatively, use carriage returns to separate the host names of the individual computers that you want to look up, or enter a partial computer name along with of the other wild card search characters.
4. (Optional) To filter out the computers that do not have Management Agent installed, check **Display only computers with Management Agent Client**.
5. Click **Run**.
6. (Optional) To view more details about the client computer in the record, right-click each record in the report, and select **View Selection**.

**Viewing the encryption status of computers that have either Drive Encryption or Removable Media Encryption installed**

The Endpoint Encryption Client Status report lets you simultaneously view the encryption status of client computers that have Drive Encryption and Removable
Media Encryption installed. You can also use the report to determine which computers in Active Directory have either Drive Encryption or Removable Media Encryption installed.

**Table 11-6** Default columns that are displayed in the Endpoint Encryption Status report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>OS</td>
<td>The name of the operating system that is currently installed on the client computer.</td>
</tr>
<tr>
<td>RME Version</td>
<td>The version of the Removable Media Encryption functionality that is currently installed on the client computer.</td>
</tr>
<tr>
<td>DE Version</td>
<td>The version of the Drive Encryption functionality that is currently installed on the client computer.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

To view the encryption status and decryption status of computers in Active Directory

1. In the navigation pane of the Management Console, expand the **Symantec Endpoint Encryption Reports** snap-in.

2. Click the **Endpoint Encryption Client Status** report.

3. In the **Enter Computer Names** field type the names of the computers whose encryption and decryption status you want to view. Use carriage returns to separate each computer name.

Alternatively, to view the encryption status and decryption status of all of the computers in Active Directory, type only the % character.
4 (Optional) To limit the scope of the report to only the computers that have the Management Agent client installed, check Display only computers with Management Agent Client.

5 Click Run.

Viewing a list of computers that currently do not encrypt files on removable media devices

The Computers not Encrypting to Removable Media Encryption report displays information about the computers that were not protected by an automatic encryption policy during the most recent check-in.

Table 11-7 Default columns that are displayed in the Computers not Encrypting to Removable Media Encryption report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
</tbody>
</table>
Table 11-7 Default columns that are displayed in the Computers not Encrypting to Removable Media Encryption report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

To view a list of computers that currently do not encrypt files on removable media devices

1 In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.

2 Click the Computers not Encrypting to Removable Media Encryption report.

3 (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select View Selection.

Viewing a list of computers whose fixed drives are currently not encrypted

The Computer with Decrypted Drives report displays information about computers that have one or more fully decrypted fixed drives. The report also lists the computers with newly installed Drive Encryption clients that have not initiated encryption.
<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the <strong>Symantec Endpoint Encryption Users and Computers</strong> snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
</tbody>
</table>
The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.
See “About the extended columns in reports” on page 199.

To view a list of computers whose fixed drives are currently not encrypted

1 In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.

2 Click the Computers with Decrypted Drives report.

3 (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select View Selection.

Viewing a list of computers whose certificates expire within a specified number of days

The Computer with Expired Certificates report displays the records of the client computers that have Certificate Authority (CA) certificates that are scheduled to expire within a specified number of days.

Table 11-9 Default columns that are displayed in the Computers with Expired Certificates report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
</tbody>
</table>
Table 11-9  Default columns that are displayed in the Computers with Expired Certificates report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

To view a list of computers whose certificates expire within a specified number of days

1  In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.

2  Click the Computers with Expired Certificates report.

3  In the Days the certificate will expire box, type number of days within which the certificates are expected to expire.

4  Click Run.

5  (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select View Selection.
Viewing a list of computers on which a specified user is registered

The Computer with Specified Users report lets you find out which computers a user is registered on. The report lets you specify more than one user, and displays the computer details that are relevant to all of them.

**Table 11-10** Default columns that are displayed in the Computers with Specified Users report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the <a href=".link">Symantec Endpoint Encryption Users and Computers</a> snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
</tbody>
</table>
Table 11-10  Default columns that are displayed in the Computers with Specified Users report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

To view a list of computers on which a specified user is registered

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Computers with Specified Users report.
3. In the Enter User Names box, type the user name that you want to search for. Use carriage returns to separate multiple user names.

   Alternatively, to view the details of any computer on which at least one user is registered, type the % character.
4. Click Run.
5. (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select View Selection.

Viewing a list of computers that do not have Drive Encryption installed

The Computers without Drive Encryption Installed report displays information of the following computers in Active Directory:

- Computers that did not have Drive Encryption installed at the most recent check-in.
- Computers that reside in a forest or on a tree that is synchronized with the Symantec Endpoint Encryption Management Server and have not checked in. These clients may or may not have Drive Encryption installed.
### Table 11-11
Default columns that are displayed in the Computers without Drive Encryption Installed report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
</tbody>
</table>
The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

To view a list of computers that do not have Drive Encryption installed

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.

2. Click the Computers without Drive Encryption Installed report.

3. (Optional) To limit the results that are displayed in the report to only the client computers that have Management Agent installed, check Display only computers with Management Agent Client.

4. (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select View Selection.

Viewing a list of computers that do not have Removable Media Encryption installed

The Computers without Removable Media Encryption Installed report displays information about the following computers in Active Directory:

- Computers that did not have Removable Media Encryption installed at the most recent check-in.

- Computers that reside in a forest or a tree that is synchronized with the Symantec Endpoint Encryption Management Server and have not checked in. These clients may or may not have Removable Media Encryption installed.

**Table 11-12** Default columns that are displayed in the Computers without Removable Media Encryption Installed report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
</tbody>
</table>
Table 11-12  Default columns that are displayed in the Computers without Removable Media Encryption Installed report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.
To view a list of computers that do not have Removable Media Encryption installed

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.

2. Click the Computers without Removable Media Encryption Installed report.

3. (Optional) To limit the results that are displayed in the report to only the client computers that have Management Agent installed, check Display only computers with Management Agent Client.

4. (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select View Selection.

Viewing a list of removable media devices that are exempted from encryption

The Device Exemptions Report displays a list of the removable media devices in Active Directory that are exempted from encryption.

Table 11-13 Default columns that are displayed in the Device Exemptions Report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>RME Exempted Product ID</td>
<td>The product ID (PID) of the removable media device that is exempted from encryption.</td>
</tr>
<tr>
<td>RME Exempted Vendor ID</td>
<td>The vendor ID (VID) of the removable media device that is exempted from encryption.</td>
</tr>
<tr>
<td>RME Device Memo</td>
<td>The optional memo text that an administrator saved.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.
To view a list of removable media devices that are exempted from encryption

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Device Exemptions Report.
3. (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select **View Selection**.

Viewing a list of computers that have not checked in within a specified number of days

The Non-Reporting Computers report displays the details of client computers that have not checked in with the Symantec Endpoint Encryption Management Server within a specified number of days. This report is useful for making sure that the data in the Symantec Endpoint Encryption database remains fresh. It also complements the lockout policy function that disables user access to computers that have not checked in by the required date and time.

**Table 11-14** Default columns that are displayed in the Non-Reporting Computers report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
</tbody>
</table>
### Table 11-14  Default columns that are displayed in the Non-Reporting Computers report *(continued)*

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether files on removable media devices are password-encrypted or certificate-encrypted.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Exclusions</td>
<td>Indicates whether a removable media device exclusion policy is enabled on the client computer.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

**To view a list of computers that have not checked in within a specified number of days**

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Non-Reporting Computers report.
3. In the Days Since Last Check-In box, type number of days for which the client computers have not checked in.
4. Click Run.
5. (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select View Selection.
Viewing the synchronization status of your Novell eDirectory

The Novell eDirectory Synchronization Status report displays information about the most recent synchronization of your Novell eDirectory.

**Note:** Symantec Endpoint Encryption 11.1.2 does not support Novell eDirectory. However, if any computers in your Novell eDirectory have Symantec Endpoint Encryption Full Disk installed 8.2.1 or an earlier version installed, the Novell eDirectory Synchronization Status report is enabled in the Symantec Endpoint Encryption Reports snap-in.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree Name</td>
<td>The name of the tree that was synchronized.</td>
</tr>
<tr>
<td>Administrator Name</td>
<td>The administrator user name in the Novell eDirectory that was used to log on to the directory service server of the tree that was synchronized.</td>
</tr>
<tr>
<td>Last Synchronization</td>
<td>The date and time of the most recent successful synchronization.</td>
</tr>
<tr>
<td>Total Computers</td>
<td>The number of computers in the Novell eDirectory that were synchronized. This number includes even computers that are not managed or protected by Symantec Endpoint Encryption.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

**To view the synchronization status of your Novell eDirectory**

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Novell eDirectory Synchronization Status report.
Viewing the percentage of computers that have fully or partly encrypted drives

The Percentage of Encrypted Endpoints report is a pie graph report that displays the percentage of computers that are fully encrypted versus the percentage of computers that not encrypted.

The report also displays a numerical representation of the compared data beneath the pie chart.

To view the percentage of computers that have fully or partly encrypted drives

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.
2. Click the Percentage of Encrypted Endpoints report.
3. (Optional) To generalize the report and consider partly encrypted drives as fully encrypted, check the Report encrypting drives as fully encrypted.
4. Click Run.

Viewing the policy details of computers that have Removable Media Encryption installed

The Removable Media Encryption Details report displays the details of the Removable Media Encryption policy settings for each reporting client.

Table 11-16 Default columns that are displayed in the Removable Media Encryption Details report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME Device Access Control</td>
<td>Indicates the level of read or write access on the removable media devices that are connected to the client computer.</td>
</tr>
</tbody>
</table>
### Table 11-16
Default columns that are displayed in the Removable Media Encryption Details report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RME Encryption Format</td>
<td>Indicates whether files on removable media devices are encrypted using the SEE RME format for Symantec Endpoint Encryption versions 11.0 and later, or the SEE RS format for Symantec Endpoint Encryption version 8.2.1. For the client computers that use a version of Removable Media Encryption earlier than 11.0.0 MP2, no value is displayed.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>Removable Media Access Utility</td>
<td>Indicates whether the Removable Media Access Utility is copied to removable media devices. This column also specifies whether the Windows version, the Mac OS X version, or both versions of the Removable Media Access Utility are copied.</td>
</tr>
<tr>
<td>RME Self-Decrypting Archives</td>
<td>Indicates whether users can create self-decrypting archives on the computers that have Removable Media Encryption installed.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

**To view the policy details of computers that have Removable Media Encryption installed**

1. In the navigation pane of the Management Console, expand the **Symantec Endpoint Encryption Reports** snap-in.

2. Click the **Removable Media Encryption Details** report.

3. (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select **View Selection**.
Viewing the encryption status of Macintosh computers that have Symantec Endpoint Encryption for FileVault installed

The Mac Computers FileVault Status report lets you view the encryption status of Macintosh client computers that have Symantec Endpoint Encryption for FileVault installed.

**Table 11-17** Default columns that are displayed in the Mac Computers FileVault Status report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>MA Version</td>
<td>The version number of the Management Agent client that is currently installed on the client computer.</td>
</tr>
</tbody>
</table>
Table 11-17 Default columns that are displayed in the Mac Computers FileVault Status report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileVault Status</td>
<td>Indicates the current state of the FileVault application. The following values are possible:</td>
</tr>
<tr>
<td>Off</td>
<td>FileVault is not currently managed by Symantec Endpoint Encryption for FileVault.</td>
</tr>
<tr>
<td>Off – Managed</td>
<td>FileVault is currently managed by Symantec Endpoint Encryption for FileVault, but has been disabled by the user.</td>
</tr>
<tr>
<td>On – Managed (with IRK)</td>
<td>FileVault is active, the Personal Recovery Key (PRK) is not stored in the Symantec Endpoint Encryption Management Server database, and the Institutional Recovery Key (IRK) policy setting is enabled.</td>
</tr>
<tr>
<td>On – Managed (with PRK)</td>
<td>FileVault is active, the Personal Recovery Key (PRK) is stored in the Symantec Endpoint Encryption Management Server database, and the Institutional Recovery Key (IRK) policy setting is disabled.</td>
</tr>
<tr>
<td>On – Managed (with PRK and IRK)</td>
<td>FileVault is active, the Personal Recovery Key (PRK) is stored in the Symantec Endpoint Encryption Management Server database, and the Institutional Recovery Key (IRK) policy setting is enabled.</td>
</tr>
<tr>
<td>Unknown</td>
<td>The FileVault encryption status is unknown, or the Symantec Endpoint Encryption for FileVault has not transmitted the information to the Symantec Endpoint Encryption Management Server.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

To view the encryption status of Macintosh computers that have Symantec Endpoint Encryption for FileVault installed

1 In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.

2 Click the Mac Computers FileVault Status report.
3 (Optional) To limit the scope of the report to only the computers that have the Management Agent client installed, check **Display only computers with Management Agent Client**.

4 (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select **View Selection**.

### Viewing the encryption status of computers that have Symantec Endpoint Encryption for BitLocker installed

The Computers with BitLocker Encryption report lets you view the encryption status of client computers that have Symantec Endpoint Encryption for BitLocker installed.

| **Table 11-18** Default columns that are displayed in the Computers with BitLocker Encryption report |
|---|---|
| **Icon** | **Description** |
| Computer Name | The host name of the client computer being monitored. |
| Group Name | The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in. |
| Last Check-in | The date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server. |
| Decrypted | The volume letters of any unencrypted volumes on the client computer. |
| Decrypting | The volume letters of any volumes that are in the process of decryption. |
| Encrypted | The volume letters of any encrypted volumes on the client computer. |
| Encrypting | The volume letters of any volumes that are in the process of encryption. |
| Hardware Encrypted Drives | Indicates whether the client computer has hardware encrypted volumes or not. |
| Encryption Type | Indicates that the volumes are encrypted by Microsoft BitLocker. |
| RME Device Access Control | Indicates the level of read or write access on the removable media devices that are connected to the client computer. |
Table 11-18  Default columns that are displayed in the Computers with BitLocker Encryption report (continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RME Encryption Format</td>
<td>Indicates whether files on removable media devices are encrypted using the SEE RME format for Symantec Endpoint Encryption versions 11.0 and later, or the SEE RS format for Symantec Endpoint Encryption version 8.2.1. For the client computers that use a version of Removable Media Encryption earlier than 11.0.0 MP2, no value is displayed.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action that is taken for automatic encryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether users can perform right-click encryption and right-click decryption of files on removable media devices (except CDs and DVDs).</td>
</tr>
<tr>
<td>Removable Media Access Utility</td>
<td>Indicates whether the Removable Media Access Utility is copied to removable media devices. This column also specifies whether the Windows version, the Mac OS X version, or both versions of the Removable Media Access Utility are copied.</td>
</tr>
<tr>
<td>RME Self-Decrypting Archives</td>
<td>Indicates whether users can create Self-Decrypting Archive files on the computers that have Removable Media Encryption installed.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

**To view the encryption status of computers that have Symantec Endpoint Encryption for BitLocker installed**

1. In the navigation pane of the Management Console, expand the **Symantec Endpoint Encryption Reports** snap-in.
2. Click the **Computers with BitLocker Encryption** report.
3. (Optional) To view more detailed information about a client computer that is listed in the report, right-click the record, and select **View Selection**.
Viewing a list of computers that received the new Web Access parameters

The **Computers that received the new Web Access parameters** report displays information about the computers on which new web access parameters were set. The administrator successfully sets the new web access parameters by issuing the Change Web Access server command from the **Symantec Endpoint Encryption Users and Computers** snap-in.

**Table 11-19** Default columns that are displayed in this report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>Displays the name of the client computer on which the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Displays the location of the client computer within the <strong>Symantec Endpoint Encryption Users and Computers</strong> snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>Displays the date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Old URL</td>
<td>Displays the URL of the earlier web service on the Symantec Endpoint Encryption Management Server before the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>New URL</td>
<td>Displays the URL of the changed web service on the Symantec Endpoint Encryption Management Server after the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Old User ID</td>
<td>Displays the earlier Active Directory user account name that was in use before the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>New User ID</td>
<td>Displays the current or changed Active Directory user account name that is in use after the Change Web Access server command was applied.</td>
</tr>
</tbody>
</table>
Table 11-19  Default columns that are displayed in this report *(continued)*

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Modified</td>
<td>Displays the most recent date and time when the Change Web Access server command was applied on that client computer.</td>
</tr>
<tr>
<td>Password</td>
<td>Displays SET if a new password is set to connect with the new web service and displays NOT SET if it is not set with a new password when the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Displays SET if a new SSL certificate was included to connect with the new web service and displays NOT SET if it was not included when the Change Web Access server command was applied.</td>
</tr>
</tbody>
</table>

**Note:** The actual columns that are displayed in the report depend upon your customization of the report.

**To view a list of computers that received the new Web Access parameters**

1. In the navigation pane of the Symantec Endpoint Encryption Manager, expand the **Symantec Endpoint Encryption Reports** snap-in.

2. Expand **Server Web Access Command Report** and click **Computers that received the new Web Access parameters**.

See “Permissions required to access reports” on page 196.

See “Viewing a list of computers connected to the Server with the new Web Access parameters” on page 235.

**Viewing a list of computers connected to the Server with the new Web Access parameters**

The **Computers connected to the Server with the new Web Access parameters** report displays information about the computers that received the new web access parameters which were issued in the Change Web Access server command, and then established connection with the server successfully using the new parameters.
Table 11-20  Default columns that are displayed in this report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>Displays the name of the client computer on which the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Displays the location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>Displays the date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>New URL</td>
<td>Displays the URL of the changed web service on the Symantec Endpoint Encryption Management Server after the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>New User ID</td>
<td>Displays the current or changed Active Directory user account name that is in use after the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Displays the most recent date and time when the Change Web Access server command was applied on that client computer.</td>
</tr>
<tr>
<td>Password</td>
<td>Displays SET if a new password was set to connect with the new web service and displays NOT SET if it is not set with a new password when the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Displays SET if a new SSL certificate was included to connect with the new web service and displays NOT SET if it was not included when the Change Web Access server command was applied.</td>
</tr>
</tbody>
</table>

**Note:** The actual columns that are displayed in the report depend upon your customization of the report.
To view a list of computers connected to Server with the new Web Access parameters

1. In the navigation pane of the Symantec Endpoint Encryption Manager, expand the **Symantec Endpoint Encryption Reports** snap-in.

2. Expand **Server Web Access Command Report** and click **Computers connected to Server with the new Web Access parameters**.

See “Permissions required to access reports” on page 196.

See “Viewing a list of computers not connected to the Server with the new Web Access parameters” on page 237.

### Viewing a list of computers not connected to the Server with the new Web Access parameters

The **Computers not connected to Server with the new Web Access parameters** report displays information about the computers that received the new web access parameters but could not establish a connection with the server using the new parameters. The parameters are distributed by the administrator using the Change Web Access server command from the Symantec Endpoint Encryption Users and Computers snap-in.

<table>
<thead>
<tr>
<th><strong>Table 11-21</strong> Default columns that are displayed in this report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Column name</strong></td>
</tr>
<tr>
<td>Computer Name</td>
</tr>
<tr>
<td>Group Name</td>
</tr>
<tr>
<td>Last Check-In</td>
</tr>
<tr>
<td>New URL</td>
</tr>
</tbody>
</table>
### Table 11-21  Default columns that are displayed in this report (continued)

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New User ID</td>
<td>Displays the current or changed Active Directory user account name that is in use after the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Displays a message that describes the problem that has occurred preventing the client computer from connecting with the Symantec Endpoint Encryption Management Server using the new Web Access parameters.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Displays the most recent date and time when the Change Web Access server command was applied on that client computer.</td>
</tr>
<tr>
<td>Password</td>
<td>Displays SET if a new password is set to connect with the new web service and displays NOT SET if it is not set with a new password when the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Certificate</td>
<td>Displays SET if a new SSL certificate was included to connect with the new web service and displays NOT SET if it is not included when the Change Web Access server command was applied.</td>
</tr>
</tbody>
</table>

**Note:** The actual columns that are displayed in the report depend upon your customization of the report.

**To view a list of computers not connected to Server with the new Web Access parameters**

1. In the navigation pane of the Symantec Endpoint Encryption Manager, expand the **Symantec Endpoint Encryption Reports** snap-in.
2. Expand **Server Web Access Command Report** and click **Computers not connected to Server with the new Web Access parameters**.

See “Permissions required to access reports” on page 196.

See “Viewing a list of computers that are redirected to another web server” on page 239.
Viewing a list of computers that are redirected to another web server

The Computers that are redirected to the other web server report displays information about those client computers on which the administrator successfully applied the new web access parameters and enable the computers to report to another web server connect to the current database. The administrator sets the appropriate parameters using the Change Web Access server command and issues the command from the Symantec Endpoint Encryption Users and Computers snap-in.

Table 11-22  Default columns that are displayed in this report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>Displays the name of the client computer on which the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>Group Name</td>
<td>Displays the location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>Displays the date and time of the most recent connection between the client computer and the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Old URL</td>
<td>Displays the URL of the earlier web service on the Management Server before the Change Web Access server command was applied.</td>
</tr>
<tr>
<td>New URL</td>
<td>Displays the URL of the changed web service on the Management Server after the Change Web Access command was applied.</td>
</tr>
<tr>
<td>Last Modified</td>
<td>Displays the most recent date and time when the Change Web Access server command was applied on that client computer.</td>
</tr>
</tbody>
</table>

Note: The actual columns that are displayed in the report depend upon your customization of the report.
To view a list of computers that are redirected to another web server

1. In the navigation pane of the Management Console, expand the **Symantec Endpoint Encryption Reports** snap-in.

2. Expand **Server Web Access Command Report** and click the **Computers that are redirected to the other web server** report.

See “Permissions required to access reports” on page 196.

See “Viewing a list of computers that received the new Web Access parameters” on page 234.

Viewing information about computers that have Opal v2 compliant drives

The Computers with Hardware Encrypted Drives report enables you to view the encryption details of client computers that have Opal v2 compliant drives.

**Table 11-23** Default columns that are displayed in the Computers with Hardware Encrypted Drives report

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Name</td>
<td>The host name of the client computer being monitored.</td>
</tr>
<tr>
<td>Group Name</td>
<td>The location of the client computer within the Symantec Endpoint Encryption Users and Computers snap-in.</td>
</tr>
<tr>
<td>Last Check-In</td>
<td>The date and time of the last connection that the client computer made with the Symantec Endpoint Encryption Management Server.</td>
</tr>
<tr>
<td>Decrypted</td>
<td>The drive letters of any unencrypted drives on the client computer.</td>
</tr>
<tr>
<td>Decrypting</td>
<td>The drive letters of any drives that are in the process of decryption.</td>
</tr>
<tr>
<td>Encrypted</td>
<td>The drive letters of any encrypted drives on the client computer.</td>
</tr>
<tr>
<td>Encrypting</td>
<td>The drive letters of any drives that are in the process of encryption.</td>
</tr>
<tr>
<td>Encryption Paused</td>
<td>The drive letters of any drives where encryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
</tbody>
</table>
### Table 11-23

Default columns that are displayed in the Computers with Hardware Encrypted Drives report *(continued)*

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decryption Paused</td>
<td>The drive letters of any drives where decryption is paused by the client administrator or due to the occurrence of a bad sector.</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Indicates whether disks are encrypted by Symantec Endpoint Encryption, Apple FileVault2, or Microsoft BitLocker.</td>
</tr>
<tr>
<td>RME Encryption Policy</td>
<td>Indicates the action is taken for automatic encryption of files on removable media devices as defined in the active policy.</td>
</tr>
<tr>
<td>RME Encryption Method</td>
<td>Indicates whether password or certificate-based encryption is allowed by the current policy in effect for files on removable media devices.</td>
</tr>
<tr>
<td>RME On-Demand Encryption</td>
<td>Indicates whether right-click encryption and decryption of files on removable media devices (except CDs and DVDs) is allowed by the active policy.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

**To view information about computers that have Opal v2 compliant drives**

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in to view the list of available reports.

2. Click the Computers with Hardware Encrypted Drives report.

See “Changing the columns that are displayed in a report” on page 198.

See “About the extended columns in reports” on page 199.

### Viewing the history of server commands

You can view all of the server commands that have ever been issued to computers that have Drive Encryption installed in the Command History report. You can either view all of the server commands in the Command History report, or you can view a the history of each unique command type in the Decrypt Drive report, the Encrypt Drive report, and the Change Web Access report.
Table 11-24  Default columns that are displayed in the three server command history reports

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of Issue</td>
<td>The date and time that the server command was issued.</td>
</tr>
<tr>
<td>Command</td>
<td>A description of the server command that was issued. This column is available only in the Command History report.</td>
</tr>
<tr>
<td>Issued By</td>
<td>The Windows domain and user name of the administrator who issued the server command.</td>
</tr>
<tr>
<td>Computer Issued From</td>
<td>The host name of the computer from which the administrator issued the server command.</td>
</tr>
<tr>
<td>Command Data</td>
<td>For the encryption and decryption commands, this column indicates the letters of the drives letters that were affected, or whether all of the drives were affected. For the Change Web Access commands, this column indicates the web server access parameters that were transmitted to the affected client computers.</td>
</tr>
</tbody>
</table>

The actual columns that are displayed in the report depend upon your customization of the report.

See “Changing the columns that are displayed in a report” on page 198.

To view the history of server commands

1 In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Server Commands snap-in.

Note: To access the Symantec Endpoint Encryption Server Commands snap-in, you must have either the Server Administrator role or the Policy Administrator role.

2 Select one of the following reports to view the required data:

- **Command History** – Displays the complete history of all server commands that were issued, regardless of the operation that was carried out.

- **Decrypt Drive** – Displays the history of server commands that were issued to decrypt drives remotely.

- **Encrypt Drive** – Displays the history of server commands that were issued to encrypt drives remotely.
■ **Change Web Access** – Displays the history of server commands that were issued to reconfigure the web server access parameters for the client computers.

3 (Optional) To view information about the client computers that were affected by a particular server command, double-click that record in the report.

**Verifying policy deployment in Active Directory**

You can use the Group Policy Management snap-in to generate a Group Policy Report. A Group Policy Report lets you verify that the Active Directory policies that you or another administrator configured, have been enforced successfully. You must configure and create a Group Policy Report for a forest or tree of your directory service before you can run it.

---

**Note:** To create a Group Policy Report, you must have either the Server Administrator role or the Policy Administrator role.

The following procedure provides instructions for creating a Group Policy Report.

**To create a Group Policy Report**

1 In the navigation pane of the Management Console, expand the Group Policy Management snap-in.

2 Expand the forest or tree for which you want to create a Group Policy Report.

3 Right-click Group Policy Results, and then click Group Policy Results Wizard.

4 On the welcome page of the Group Policy Results Wizard window, click Next.

5 On the Computer Selection page, select one of the following options:

   ■ To create a Group Policy Report for the current computer, select This computer.

   ■ To create a Group Policy Report for another client computer in Active Directory, select Another Computer, and then type the name of the computer in the text box.

     Alternatively, select Another Computer and then click Browse, search for the desired computer in Active Directory and select it.

6 (Optional) To configure the report to display only the policies that apply to registered users on the selected computer, check Do not display policy settings for the selected computer in the results (display user policy settings only).

7 Click Next.
On the User Selection page, select one of the following options:

- To display user policy settings in the report, select **Display policy settings for**, and then choose whether you want to view the policy settings for the current logged in user (Current user option) or for another registered user on the selected client computer (Select a specific user option).
  
  If you select **Select a specific user**, you must also choose a user from the list.

- To prevent the report from displaying user policy settings, select **Do not display user policy settings in the results (display computer policy settings only)**.
  
  Do not select this option if you checked **Do not display policy settings for the selected computer in the results (display user policy settings only)** on the Computer Selection page.

9 Click **Next** and then review the report configuration on the Summary of Selections page.

10 To confirm the report configuration, click **Next**.

11 Click **Finish**.

The following procedure provides instructions for running a Group Policy Report to verify policy deployment.

**To verify policy deployment in Active Directory**

1 In the navigation pane of the Management Console, expand the **Group Policy Management** snap-in.

2 Expand the forest or tree for which you want to create a Group Policy Report.

3 Expand the **Group Policy Results** section in the selected forest or tree.

4 Click the Group Policy Report that you want to run.

5 Navigate through the available tabs in the report.

You can click each of the rows in the **Summary** and **Settings** tabs to expand or collapse them. Use them to drill down to the policy settings that you want to verify.

**Creating and editing custom reports**

This section contains the following topics:

- Creating custom reports
- Editing custom reports
Creating custom reports

Symantec Endpoint Encryption lets you create your own reports in addition to the default reports that are available in the Management Console. You can edit these custom reports at any time.

**Note:** To access custom reports, the user must have administrative rights. Local users cannot access custom reports.

**To create a custom report**

1. In the navigation pane of the Management Console, expand the **Symantec Endpoint Encryption Reports** snap-in.

2. (Optional) Right-click **Custom Reports**, and select **New Report Container** to create a new folder in the navigation pane where you can create reports.

   Alternatively, if there are already one or more containers, right-click a container and select **New Report Container** to create a subfolder inside it.

3. To create a new report directly under **Custom Reports**, right-click **Custom Reports**, and select **New Report**.

   Alternatively, to create a new report inside a different container (if any), right-click the container, and select **New Report**.

4. In the **Query Editor** dialog box, use the various text boxes and check boxes to define the query condition for your custom report.

5. Click **Save**.

6. In the **New Report Name** dialog box, type a name for your report in the text box.

7. Click **OK**.

8. In the navigation pane, right-click the new report that you created, and select **Configure Columns Displayed**.

   See “About the extended columns in reports” on page 199.

9. In the **Select Columns** dialog box, check the columns that you want the report to display.

10. (Optional) If you want Symantec Endpoint Encryption to adjust the column widths for you, check **Automatically adjust column width**.

11. Click **OK**.
Editing custom reports

You modify the query conditions in the custom reports that you or another administrator created, at any time. The following procedure provides instructions for editing a custom report.

To edit a custom report

1. In the navigation pane of the Management Console, expand the Symantec Endpoint Encryption Reports snap-in.

2. Expand the Custom Reports section, and any required report containers.

3. Right-click the custom report that you want to edit, and select Edit Report Query.

4. In the Query Editor dialog box, use the text boxes and check boxes to make the necessary modifications to the report query.

5. To overwrite the existing custom report, click Save.
   Alternatively, to save the modified query as a new custom report with a different name, click Save As.

6. (Optional) To change the columns that are displayed in the report, right-click the modified custom report and select Configure Columns Displayed. Use the Select Columns dialog box to customize the columns that are displayed in the report.

   See “About the extended columns in reports” on page 199.
Providing recovery support to your users

This chapter includes the following topics:

- About Symantec Endpoint Encryption Help Desk Recovery program
- Providing Help Desk Recovery user assistance for Symantec Endpoint Encryption clients
- Providing One-Time Password user assistance for legacy Symantec Endpoint Encryption clients
- Providing Whole Disk Recovery Token user assistance for client computers
- Providing Help Desk Recovery assistance for the Symantec Endpoint Encryption for FileVault users
- Providing Help Desk Recovery assistance for the Symantec Endpoint Encryption for BitLocker users
- Best practices for recovering data
- Recovering the Macintosh encrypted disk

About Symantec Endpoint Encryption Help Desk Recovery program

With the Help Desk Recovery program, you can provide recovery support to the client users when they lose their password or are locked out at preboot. This assistance provides the user with a Response Key or a One-Time Password which allows the user to temporarily authenticate on their encrypted computer.

To use the Help Desk Recovery program, you must:
■ Use a Manager Computer that has the Help Desk Recovery Program snap-in installed.

■ Log on to the Manager Computer using a Windows account that has been provisioned with read access to the Symantec Endpoint Encryption database. You can also log on to the Management Console using SQL database credentials that let you read the Symantec Endpoint Encryption database.

■ Know the Management Password.

Based on the connectivity of the client with Symantec Endpoint Encryption Management Server, there are two methods of recovery:

■ Online Recovery
  Online method of recovery is possible when the client establishes a connection with Symantec Endpoint Encryption Management Server after installation. The server receives data about the client that are required to generate the Response Key in the future. Help Desk Recovery requires minimum authentication information from the client computer.

■ Offline Recovery
  Offline method of recovery is required when the client has never communicated with Symantec Endpoint Encryption Management Server after installation. The server does not have any information about the client that is required to generate the Response Key. Help Desk Recovery, therefore, requires a Challenge Key for authentication from the client computer. However, the information is stored in the server for future authentication and requires minimum authentication the next time the Help Desk Recovery assistance is used.

A few terms that are used while you communicate with the client user and retrieve the Response Key for a client computer are:

■ Computer identity
  The name of the client computer with the domain name. Help Desk Recovery program requires this information to verify the computer record in the server database.

■ Sequence number
  Sequence number is used to synchronize a client with the server. Help Desk Recovery program requires this information to generate the Response Key or One-Time Password.

■ Challenge Key
  A public key that the client generates using the public key of the server. Help Desk Recovery program requires this information to authenticate a client that has never communicated with the server.

■ Checksum
A two-character value that appears for the Response Key and the Challenge Key. Checksum helps to verify that the Challenge Key has been communicated correctly to the help desk administrator or the Response Key to the user. A matching checksum confirms that the Challenge Key on the server side or the Response Key on the client side have been entered correctly.

■ Personal Recovery Key
An alphanumeric string that is automatically generated when you enable FileVault on a Macintosh client computer. When the client-server communication is established, the Personal Recovery Key is sent to the server. The Personal Recovery Key is used for recovery when Symantec Endpoint Encryption for FileVault user loses their password or is locked out at preboot.

■ Institutional Recovery Key
FileVault supports an Institutional Recovery Key in addition to the Personal Recovery Key. The Institutional Recovery Key is a single key that can be used to unlock the encrypted Macintosh systems in the company or a group.

■ Bitlocker Recovery Key
A BitLocker Recovery Key is a key that is created when you turn on BitLocker encryption for the first time on the client computer where Symantec Endpoint Encryption for BitLocker is installed. When the client-server communication is established, the BitLocker Recovery Key is sent to the server. The BitLocker Recovery Key is used for recovery when the Symantec Endpoint Encryption for BitLocker user forgets their PIN or is locked out at preboot.

About the Symantec Endpoint Encryption web-based Help Desk Recovery console
The Help Desk Recovery feature that was available as a Symantec Endpoint Encryption Management Server snap-in is now also available as a web-based Help Desk Recovery console. The web-based Help Desk Recovery console is an administrative, browser-based, interface to manage recovery of encrypted clients that are installed as part of the Symantec Endpoint Encryption Management Server infrastructure. The web-based Help Desk Recovery console supports Internet Explorer 11 or later, and Chrome 54 or later.

Using the web-based Help Desk Recovery console, help desk administrators can now recover locked out computers without installing the Symantec Endpoint Encryption Manager console. However, only users with the Helpdesk server role can access web-based Help Desk Recovery console. The web-based Help Desk Recovery console supports all of the recovery methods available in the Help Desk Recovery program that is available as a Symantec Endpoint Encryption Management Server snap-in.

Administrators can also deploy multiple Symantec Endpoint Encryption Management Server with a same database and configure the Help Desk Recovery
console to run behind a load balancer. You can also configure a custom URL for the Help Desk Recovery console with a load balancer using the Symantec Endpoint Encryption Configuration Manager interface. Help Desk Recovery uses challenge-response authentication method to let users recover their passwords or unlock a user account. The Help Desk Recovery offers data recovery service only to enterprise users managed by Symantec Endpoint Encryption Management Server.

For more information on the Symantec Endpoint Encryption web-based Help Desk Recovery console, see the Symantec Endpoint Encryption Help Desk Recovery online help that is integrated with the Help Desk Recovery console.

Providing Help Desk Recovery user assistance for Symantec Endpoint Encryption clients

You can select the Help Desk Recovery option to provide recovery assistance to the users on client computers that have Symantec Endpoint Encryption 11.1.2 installed.

Before you select this recovery option, ask the user the following questions:

■ Is the screen labeled as Help Desk Recovery?
■ Is the screen displaying a Computer and Sequence number?

Based on the communication status of the client computer with Symantec Endpoint Encryption Management Server, you provide either online recovery assistance or offline recovery assistance. For offline recovery assistance, a user selects the Advanced Help Desk Recovery option and provides you with the Challenge Key for authentication.

When you type the Challenge Key, a two-digit checksum appears at the end of the box. Similarly, when the user types the Response Key on the client screen, a checksum appears at the end of the box. Ask the user to read the checksum to you. Ensure that the checksum for the Challenge Key or the Response Key on the client side matches with the checksum on the server side.

Note: If the user is unable to complete the Help Desk Recovery process even after multiple attempts, you can recommend that a client administrator authenticate for recovery.
To use Help Desk Recovery

1. In the left pane of Symantec Endpoint Encryption Manager, click **SEE Help Desk > Help Desk Recovery Program**.
2. On the Welcome page, click **Next**.
3. Type the current management password in the **Enter the SEE management password provided by your administrator** box, and click **Next**.
4. On the **Help Desk Recovery Options** page, select **Help Desk Recovery**, and then click **Next**.
5. On the **Help Desk Recovery** page, do one of the following:
   - If the client computer requires the online method of recovery, type the information that the user provides in the **Computer** and **Sequence Num** boxes.
   - If the client computer requires the offline method of recovery, type the information that the user provides in the **Computer**, **Sequence Num**, and **Challenge Key** boxes. Match the checksum to ensure that you have typed the Challenge Key correctly.
6. Click **Next**.
7. From the **Help Desk Recovery Program – Response Key** page, read aloud the string of characters that you see in the **Response Key** box to the user. Match the checksum to ensure that the user has typed the Response Key correctly.
8. Do one of the following:
   - Click **Yes** if the user has successfully recovered the encrypted computer, and then click **Next**.
   - Click **No** if the user is unable to recover the encrypted client computer, and then click **Next**.
9. Do one of the following:
   - If you clicked **Yes** in the previous page, click **Finish** to close the Help Desk Recovery program.
   - If you clicked **No**, the wizard takes you to the beginning of the Help Desk Recovery program so that you can reconfirm the information that you have entered. For online clients, you can ask the user to try the Advanced Help Desk Recovery option and use the Challenge Key to generate the Response Key.
Providing One-Time Password user assistance for legacy Symantec Endpoint Encryption clients

You can select the One-Time Password options to provide recovery assistance to the users on the client computers that have versions of Symantec Endpoint Encryption earlier than 11.1.2.

You can use one of the following methods of recovery:

■ The online method of recovery is used for the clients that communicate with Symantec Endpoint Encryption Management Server after installation of Symantec Endpoint Encryption.

■ The offline method of recovery is used for the clients that have never communicated with Symantec Endpoint Encryption Management Server after installation of Symantec Endpoint Encryption.

Before you select the Legacy OTP Recovery – Online or the Legacy OTP Recovery - Offline options, you must ask the user the following questions:

■ Do the Online and Offline options appear on the screen?

■ Is the default option that is selected on the screen Online or Offline?

When you type the Challenge Key for the offline method of recovery, a two-digit checksum appears at the end of the box. Similarly, when the user types the Response Key on the client screen, a checksum appears at the end of the box. Ask the user to read the checksum aloud. Ensure that the checksum for the Challenge Key or the Response Key on the client side matches with the checksum on the server side.

Note: If the user is unable to complete the recovery process even after multiple attempts, you can recommend that a client administrator authenticate for recovery.

To provide One-Time Password user assistance for online legacy clients

1 In the left pane of Symantec Endpoint Encryption Manager, click SEE Help Desk > Help Desk Recovery Program.

2 On the Welcome page, click Next.

3 Type the current Management Password in the Enter the SEE management password provided by your administrator box, and click Next.

4 On the Help Desk Recovery Options page, select Legacy OTP Recovery - Online, and then click Next.

5 On the One-Time Password Program – Online Method page, do the following:
To provide One-Time Password user assistance for offline legacy clients

1 In the left pane of Symantec Endpoint Encryption Manager, click SEE Help Desk > Help Desk Recovery Program.

2 On the Welcome page, click Next.

3 Type the current Management Password in the Enter the SEE management password provided by your administrator box, and click Next.

4 On the Help Desk Recovery Options page, select Legacy OTP Recovery - Offline, and then click Next.

5 On the One-Time Password Program – Offline Method page, do the following:
Type the identifier that the user provides in the Personal Identifier box. This information is mandatory to retrieve a One-Time Password.

Type the Challenge Key that the user provides in the Challenge Key boxes. Match the checksum to ensure that you have typed the Challenge Key correctly. This information is mandatory to retrieve a One-Time Password.

6 Click Next.

7 From the Help Desk Recovery Program – Response Key page, read aloud the string of characters that you see in the Response Key box to the user. Match the checksum to ensure that the user has typed the Response Key correctly.

8 Do one of the following:
   ■ Click Yes if the user has successfully recovered the encrypted computer, and then click Next.
   ■ Click No if the user is unable to recover the encrypted client computer, and then click Next.

9 Do one of the following:
   ■ If you clicked Yes in the previous page, click Finish to close the Help Desk Recovery program.
   ■ If you clicked No, the wizard takes you to the beginning of the Help Desk Recovery program so that you can reconfirm the information that you have entered.

Providing Whole Disk Recovery Token user assistance for client computers

You can provide Whole Disk Recovery Token user assistance for a client computer if:
   ■ Symantec Endpoint Encryption Management Server identifies a client that is running Mac OS X on the computer and has a version of Symantec Endpoint Encryption Full Disk 8.2.1 or earlier.
   ■ The Symantec Endpoint Encryption Management Server database is connected to Symantec Encryption Management Server and the Symantec Encryption Desktop clients require Whole Disk Recovery Token for recovery.

Before you select this option, ask the user the following questions:
   ■ Is the screen displaying a Machine ID, Disk ID, or UUID?
Is the client running Mac OS X on the computer and does it have a version of Symantec Endpoint Encryption Full Disk 8.2.1 or earlier?

To provide WDRT user assistance

1. In the left pane of Symantec Endpoint Encryption Manager, click **SEE Help Desk > Help Desk Recovery Program**.

2. On the Welcome page, click **Next**.

3. Type the current Management Password in the **Enter the SEE management password provided by your administrator** box, and click **Next**.

4. On the **Help Desk Recovery Options** page, select **WDRT Recovery**, and then click **Next**.

5. On the **Whole Disk Recovery Token Program** page, do the following:
   - Type the Machine ID, Disk ID, or UUID that the user provides in the **Machine/Disk ID** box. This information is mandatory to retrieve Whole Disk Recovery Token.
   - Type the name of the user in the **User Name** box.

6. Click **Next**.

7. From the **Whole Disk Recovery Token Program** page where the token characters appear, read aloud the characters of the token to the user. Ask the user to type the characters correctly.

8. Do one of the following:
   - Click **Yes** if the user has successfully recovered the encrypted computer, and then click **Next**.
   - Click **No** if the user is unable to recover the encrypted client computer, and then click **Next**.

9. Do one of the following:
   - If you clicked **Yes** in the previous page, click **Finish** to close the Whole Disk Recovery Token program.
   - If you clicked **No**, the wizard takes you to the beginning of the Whole Disk Recovery Token program so that you can reconfirm the information that you have entered.
Providing Help Desk Recovery assistance for the Symantec Endpoint Encryption for FileVault users

You can select the Help Desk Recovery option to provide recovery assistance to the Macintosh users that have Symantec Endpoint Encryption for FileVault installed.

Before you select this recovery option, ask the user the following:

- Their user name
- The serial number of the encrypted Macintosh computer

If the communication is established between Macintosh client computer and Symantec Endpoint Encryption Management Server, you can provide the Personal Recovery Key to the user for access recovery.

To use Help Desk Recovery

1. In the left pane of Symantec Endpoint Encryption Manager, click SEE Help Desk Recovery > Help Desk Recovery Program.
2. On the Welcome page, click Next.
3. Type the current management password in the Enter the SEE management password provided by your administrator box, and click Next.
4. On the Help Desk Recovery Options page, select Mac Personal Recovery Key Program, and then click Next.
5. On the Mac Personal Recovery Key Program – User page, do the following:
   - In the User Name box, type the name of the user for which you want to provide the Personal Recovery Key.
     Alternatively, to view all of the users, type the % character.
   - Click Search.
   - In the Users List box, the user details appear in the following boxes:
     - User Name
     - Mac Serial ID
     - Last Check-In
   - Select the appropriate user and click Next.
Providing Help Desk Recovery assistance for the Symantec Endpoint Encryption for BitLocker users

You can select this Help Desk Recovery option to provide recovery assistance to the users that have Symantec Endpoint Encryption for BitLocker installed.

To use this recovery option, you need the BitLocker Recovery Key ID, which the user provides.

If communication is established between client computer and Symantec Endpoint Encryption Management Server, you can provide the BitLocker Recovery Key to the user for access recovery.

To use Help Desk Recovery

1. In the left pane of Symantec Endpoint Encryption Manager, click SEE Help Desk > Help Desk Recovery Program.

2. On the Welcome page, click Next.

3. In the Enter the SEE management password provided by your administrator box, type the Management Password, then click Next.
4 On the Help Desk Recovery Options page, select BitLocker Recovery Key, and then click Next.

5 On the BitLocker Recovery Key - BitLocker Recovery Key ID page, enter the BitLocker Recovery Key ID that the user provides.

6 Click Next.

7 From the BitLocker Recovery Key - BitLocker Recovery Key ID page, read aloud the digits that you see in the BitLocker Recovery Key box to the user.

8 Do one of the following:
   - Click Yes if the user has successfully recovered the encrypted computer, and then click Next.
   - Click No if the user is unable to recover the encrypted client computer, and then click Next.

9 Do one of the following:
   - If you clicked Yes on the previous page, click Finish to close the BitLocker Recovery Key page.
   - If you clicked No, the wizard returns you to the BitLocker Recovery Key - BitLocker Recovery Key ID page so that you can confirm the information that you have entered.

Best practices for recovering data

Creating a customized Windows Preinstallation Environment for data recovery

When an encrypted disk fails to start the Windows operating system, recovery of data becomes the primary goal. Creating a customized Windows Preinstallation Environment (Windows PE) CD or UFD (USB flash drive) provides a bootable recovery tool that can be used for rescue purposes.

You can use a customized Windows PE CD or UFD in the following ways:
   - To restore the previous master boot record (MBR) of the client computer after you restore the computer from a volume backup.
   - To recover the preboot screen of the client computer when a user fails to authenticate at preboot or the preboot screen is unavailable.
   - To decrypt an encrypted disk using the client administrator authentication, Help Desk Recovery (for managed clients), or Advanced Help Desk Recovery (for unmanaged clients).
A customized Windows PE CD or UFD is the only way to recover your data when you cannot start your operating system. As a best practice, you must create the customized Windows PE CD or UFD immediately after installing the client software. To learn how to create a customized Windows PE CD or UFD, see Windows PE Recovery Tools for Symantec Endpoint Encryption 11.0.0.

Recovering the Macintosh encrypted disk

When a Macintosh encrypted disk fails to start the Apple Mac OS X operating system, recovery of data becomes the primary goal. Refer to the Apple user community and knowledgebase for recovering the Macintosh encrypted disk.
Recovering the Macintosh encrypted disk
Upgrading clients to Symantec Endpoint Encryption 11.1.2

This chapter includes the following topics:

■ About upgrading your Microsoft Windows clients
■ Before upgrading your Microsoft Windows clients
■ Upgrading your Microsoft Windows clients
■ Using Group Policy Objects when upgrading Microsoft Windows clients
■ Upgrading Symantec Endpoint Encryption for FileVault clients

About upgrading your Microsoft Windows clients

You can upgrade your client computers to Symantec Endpoint Encryption 11.1.2. The upgrade process lets you upgrade your client computers to the latest version of encryption products without decrypting your computers. Symantec Endpoint Encryption keeps your user data encrypted and retains the relevant metadata that it requires.

Symantec Endpoint Encryption 11.1.2 supports client upgrades from the following earlier products:

■ Symantec Endpoint Encryption 8.2.1
■ Symantec Endpoint Encryption 11.0.x
■ Symantec Encryption Desktop 10.3.2 MP4 for Windows or later
You must run the Symantec Endpoint Encryption Client installation package to complete the upgrade of the client computer. You upgrade the clients by running `msiexec` commands.

The installer first checks the drive to determine if it can successfully upgrade. If the check passes, it backs up the metadata that is necessary for data decryption. It also preserves certain data such as preboot, drivers, and volume files so that it can keep the disk’s I/O functions operational during the upgrade process.

After you upgrade, when the user restarts the computer the first time, preboot authentication is bypassed and the computer boots to Microsoft Windows. After the user logs on to Microsoft Windows for the first time, the user account is automatically registered with the client. After the next restart, the user can enter these credentials for preboot authentication. If the GPO or native policy prevents automatic registration, then preboot authentication continues to be bypassed.

If the client cannot connect to the Symantec Endpoint Encryption Management Server, it uses the policy configuration that you define in the installation MSI files. Later, if the client connects to the Symantec Endpoint Encryption Management Server, it then synchronizes its policies with the server's native policies or GPO policies.

After upgrade, auto-encryption starts on the non-encrypted partition or disk according to the encryption policy that is defined in installer (Auto-Encrypt Boot Disk/All Disk). It will have the same encryption parameters (AES cipher strength, block cipher mode) that was present with the already encrypted partitions/disk before the upgrade.

**Note:** When you upgrade the Symantec Endpoint Encryption Client, you must also upgrade any additional features that are installed, such as the Autologon Utility and the Windows Password Reset Utility.

**About the version 11.0.x upgrade scenario**

As of Symantec Endpoint Encryption 11.1.2, the Symantec Endpoint Encryption Client installation package upgrades all of the client features together. You no longer have to upgrade Management Agent, Drive Encryption, and Removable Media Encryption separately.

**About the version 8.2.1 in-place upgrade scenario**

In an in-place upgrade scenario, you first upgrade the Symantec Endpoint Encryption Management Server to the latest version. After you upgrade the server, you use it to generate the new Symantec Endpoint Encryption 11.1.2 client installation files. You then use these files to upgrade your existing clients to the latest version.
**Note:** You can still use your upgraded Symantec Endpoint Encryption Management Server to manage Symantec Endpoint Encryption 8.2.1 client computers.

**About the version 8.2.1 migration scenario**

In a migration scenario, you use two management servers. You keep your existing Symantec Endpoint Encryption 8.2.1 Management Server and you install a new Symantec Endpoint Encryption Management Server 11.1.2 on another computer. This approach lets you manage clients separately. You can manage Symantec Endpoint Encryption 8.2.1 clients on the Symantec Endpoint Encryption 8.2.1 server. You can manage Symantec Endpoint Encryption 11.1.2 clients on Symantec Endpoint Encryption Management Server 11.1.2. Over time, you can then migrate your previous clients to report to Symantec Endpoint Encryption Management Server 11.1.2.

To migrate, you first install the new Symantec Endpoint Encryption Management Server on a new computer. You then use it to generate the new client MSI files and then deploy them on the client computer. After the client computer is upgraded it reports to the new Symantec Endpoint Encryption Management Server.

**Note:** Although the client computer stops reporting to the Symantec Endpoint Encryption 8.2.1 server, the server may still keep a record of the client computers. However, the clients enforce their new policy settings and report to the new Symantec Endpoint Encryption Management Server once they establish a connection to it.

**About the Symantec Encryption Desktop 10.3.2 in-place upgrade scenario**

In an in-place upgrade scenario, you can upgrade a Symantec Encryption Desktop client from version 10.3.2 MP4 or later to Symantec Endpoint Encryption 11.1.2 without needing to decrypt the disk.

**Note:** Upgrades to Symantec Endpoint Encryption might fail if the disk partition sizes were modified after the disk was encrypted using Symantec Encryption Desktop.

When you upgrade and install Drive Encryption, only the encrypted data and the metadata that is required to decrypt is migrated. Other data, such as the data for registered users, self-recovery data, and administrators are not migrated. Your users must register with Symantec Endpoint Encryption after the upgrade. The upgraded computer's state is the same as a computer with a new installation of Symantec Endpoint Encryption, except that the disk is already encrypted.
Before upgrading your Microsoft Windows clients

Consider the following before upgrading your clients:

■ Back up your data.
   As with any upgrade procedure involving encryption products, there is always the risk that unexpected problems can interrupt the upgrade process. Symantec recommends that you always back up your data before you attempt an upgrade.

■ If you upgrade a client using a Symantec Endpoint Encryption Client installation package that was created using a different Symantec Endpoint Encryption Management Server, the Help Desk Recovery feature stops working as the client computer does not exist in the new server’s database. After the upgrade is complete, ensure that the client checks in with Symantec Endpoint Encryption Management Server. Then, disable and re-enable the Help Desk Recovery feature through the policy settings.

■ Saved all of your work and closed any open files.

■ Closed any third-party programs that read or write to the disk or read or write to removable media.

■ Dismounted and disconnected any removable media from the client computer.

■ Ensured that the disk is either completely encrypted or decrypted. If encryption or decryption is in progress, wait until the disk is completely encrypted or decrypted.

■ The system requirements for upgrades also include all of the standard Symantec Endpoint Encryption 11.1.2 system requirements.

■ Your environment must have Symantec Endpoint Encryption Management Server 11.1.2.

■ Ensure that you have installed all of the latest Windows Updates from Microsoft.

■ Version 1 hardware-encrypted Opal drives are not supported. If you have v1 Opal Drives, they must be software-encrypted. Opal drives remain software encrypted and are not converted to hardware encryption.

■ You cannot upgrade partially-encrypted drives.

■ You cannot upgrade partially-encrypted partitions.

■ You cannot upgrade disks with more than ten logical partitions.

■ You cannot upgrade if encryption or decryption is still in progress

■ Dual Boot is not supported
Symantec Endpoint Encryption 11.1.2 does not support upgrades from CPA releases of Symantec Encryption Desktop 10.3.2 for Windows

**Special considerations before you upgrade 8.2.1 client computers**

Consider the following before upgrading your 8.2.1 clients:

- Managing Symantec Endpoint Encryption 11.1.2 clients with a Symantec Endpoint Encryption 8.2.1 server is not supported.
  - Managing Symantec Endpoint Encryption 8.2.1 clients with a Symantec Endpoint Encryption Management Server 11.1.2 server is supported.

- Do not deploy Symantec Endpoint Encryption 8.2.1 policies to 11.1.2 clients.
  - You cannot manage 11.1.2 clients with a Symantec Endpoint Encryption 8.2.1 server. Make sure that you configure your client to only report to, and download data from the 11.1.2 server. After you upgrade a client to 11.1.2, only 11.1.2 policies can apply to it.

- The upgrade does not preserve policy settings during the upgrade. Instead, the install policy settings from the Symantec Endpoint Encryption 11.1.2 installers take effect after the upgrade. They take effect until the client can connect to Symantec Endpoint Encryption Management Server to retrieve policies.

- Randomly generated client data is refreshed
  - The randomly generated Machine IDs, or Disk IDs, policies, and client administrators are removed and refreshed during the upgrade. The Machine IDs and Disk IDs may be reported twice during the upgrade process. This behavior indicates that the IDs have been modified. This behavior is expected.

- Removable Media Encryption supports the 8.2.1 RS encryption format. The upgrade preserves your users' Removable Storage settings. After you upgrade to Removable Media Encryption you can access RS-encrypted data through the same authentication methods that you used with Removable Storage.

- Hidden and system partitions are now encrypted in 11.1.2. After you upgrade a client computer from the 8.2.1 version to the 11.1.2 version of Symantec Endpoint Encryption, when a user restarts the computer and logs on to Windows, almost immediately messages appear. The notifications are for the start and completion of encryption. The hard disk is not being re-encrypted. These notifications refer to the hidden and system partitions. This behavior is normal. However, the partitions are small, the process is quick, and the messages are fleeting; therefore, some users find the messages confusing. To read the messages, a user can use the Windows Event Log Viewer. They should look for messages such as, "Encryption started on boot drive by the Drive Encryption service."
Be aware that when upgrading from legacy versions, the upgrade does not preserve authentication data. The users must re-register.

Be aware that after the upgrade of legacy versions, smart card users must re-enroll to be able to authenticate to preboot.

**Data handling for 8.2.1 client upgrades**

The upgrade preserves the following data:

- The workstation encryption keys (WEK) and disk encryption keys (DEK)
- The encryption status
- The original Master Boot Record (MBR)

The Removable Media Encryption upgrade preserves the following:

- Default Password
- Session Password 1
- Session Password 2
- Default Password Memo
- Session Password 1 Memo
- Session Password 2 Memo
- The Default Certificate information
- The “user choice” feature’s settings

The upgrade changes the following:

- The Drive Encryption policy settings. These settings include Single-Sign-on (SSO), Drive Encryption Self-Recovery, and Help Desk Recovery settings
- The client administrator credentials

All other data is removed. This data includes your existing user records. After the upgrade, each user must log on to Microsoft Windows at least once to register for preboot authentication.

**Special considerations when upgrading a Symantec Encryption Desktop 10.3.2 client computer**

Consider the following before upgrading your 10.3.2 clients:

- When upgrading from 10.3.2, the clients must run Symantec Encryption Desktop 10.3.2 MP4, or above.
- Symantec Encryption Desktop Drive Encryption encrypted removable disks and encrypted USB drives are not upgraded.
You must first decrypt your removable disks, and drives before you upgrade.

- You cannot upgrade to Symantec Endpoint Encryption for BitLocker while the Symantec Drive Encryption component of Symantec Encryption Desktop is enabled.

The following 10.3.2 Symantec Encryption Desktop components are unaffected by the upgrade process. These components continue to run and report to the 3.3.2 Symantec Encryption Management Server and can run in parallel with Symantec Endpoint Encryption:

- Symantec Desktop Email Encryption
- Symantec File Share Encryption
- PGP Shredder
- PGP Viewer
- PGP ZIP
- Virtual Disk

- Be aware that when upgrading from legacy versions, the upgrade does not preserve authentication data. The users must re-register.

- Be aware that after the upgrade of legacy versions, smart card users must re-enroll to be able to authenticate to preboot.

**Using the re-encrypt command after upgrading 10.3.2 clients:**

The eedAdminCli includes a new command that lets you re-encrypt the disk using a new session key. This command changes the block cipher mode from PlumbCFB to CBC.

The command is:

```
--re-encrypt
```

For example:

```
eedAdminCli.exe --re-encrypt --disk <disk_id> --au <client_Administrator Name> --ap <client_Administrator passphrase>
```

Consider the following:

- The re-encrypt command only changes the block cipher mode from PlumbCFB to CBC (zero to three). It does not change the AES Strength of the disk which is already encrypted.

- Re-encryption is blocked for new 11 clients and all other clients that are upgraded from 8.2.1 or 11.0.x.

- Re-encryption works only at the time that the fully encrypted clients are upgraded. After the block cipher mode is changed, the command will not run.
The client administrator cannot trigger decryption until after the re-encryption process finishes. However the users can pause and resume the re-encryption process.

The status message: “re-encryption is in progress” status is displayed for the command line interface as well as in the user interface.

The Symantec Endpoint Encryption Management Console does not display any information for the re-encryption process. However, an audit event is sent to the server to indicate the start and completion of the re-encryption process.

Upgrading your Microsoft Windows clients

You can use the command line to upgrade clients to specify an output log file that you can use to troubleshoot any installation problems.

Note: When upgrading 10.3.2 client computers, decrypt your removable disks and drives before you upgrade.

To upgrade the client computers:

1. Ensure that the client computer has a stable power supply. A power failure might interrupt the upgrade process and cause it to fail.
2. Back up the computer and its data before you attempt to upgrade.
3. Confirm that the client computer meets the system requirements to run the Symantec Endpoint Encryption Client software.
   See “Creating a Symantec Endpoint Encryption Client installation package” on page 72.
5. Copy the installation .MSI file to the local hard disk of the computer on which you want to perform the upgrade.
   - If the computer's operating system is 32-bit, copy the SEE Client.msi file.
   - If the computer's operating system is 64-bit, copy the SEE Client x64.msi file.
**Note:** If you upgrade a client using a Symantec Endpoint Encryption Client installation package that was created using a different Symantec Endpoint Encryption Management Server, the Help Desk Recovery feature stops working as the client computer does not exist in the new server's database. After the upgrade is complete, ensure that the client checks in with Symantec Endpoint Encryption Management Server. Then, disable and re-enable the Help Desk Recovery feature through the policy settings.

6. Depending on the version of Microsoft Windows, do one of the following:

   **On Windows 7:**
   - Click **Start > All Programs > Accessories**.
   - Right-click **Command Prompt** and select **Run as administrator**.

   **On Windows 8.x:**
   - From the **Start** screen, access the **Apps** menu.
   - In the **Windows System** section, right-click **Command Prompt** and select **Run as administrator**.

   **On Windows 10:**
   - Click **Start > All Apps**.
   - In the **Windows System** section, right-click **Command Prompt** and select **Run as administrator**.

   If you are prompted, enter the credentials of a domain administrator account.

7. In the Command Prompt window, enter the following:

   `MSIEXEC /i "[path]\msifile" /l*v "[logpath]\logfile"`

   Where `\msifile` represents the path and name of the MSI file, and `]\logfile` represents the path and name of the output log file.

   **Note:** To complete a silent upgrade, append the command with the `CONDITION_NOUI=1` parameter.

   **Note:** Be aware that `/qn` and `/qb` modes are supported only while upgrading from an earlier version of 11.1.x. Do not use the `CONDITION_NOUI=1` parameter in this scenario.
8  When prompted, close the **Command Prompt** window and restart the computer.

**Note:** If Autologon is installed before the upgrade, it is uninstalled during the upgrade process. To re-enable it, you must reinstall the `autologon.msi` that you created using the new 11.1.0 server. When the installation is complete, restart the client computer.

9  Depending on the previous version of the client, do one of the following:

<table>
<thead>
<tr>
<th>On 11.X.X computers:</th>
<th>If you have Drive Encryption with Opal v2 compliant drives, complete the steps in the section, <em>Upgrading Drive Encryption with Opal v2 compliant drives.</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>On 8.2.1 computers</td>
<td>8.2.1 - If you upgrade to the Removable Media Encryption feature, you should be able to use the normal authentication method to access the data that was previously encrypted by Removable Storage.</td>
</tr>
</tbody>
</table>

**Upgrading Drive Encryption with Opal v2 compliant drives**

If you have existing Opal v2 compliant drives that are already encrypted by Symantec Endpoint Encryption, during upgrade those drives are not converted automatically from drives that are software encrypted to drives that are hardware encrypted. You must follow this procedure to manually convert the drives.

For more information on the Drive Encryption policy options, see the Symantec Endpoint Encryption Management Server online Help.

If the drive meets the qualifying conditions and the drive is successfully provisioned, the drive is hardware encrypted. It displays a status of “Hardware Encrypted” in reports and in the consoles. If the qualifying conditions are not met or if provisioning fails, the drive is software encrypted by Drive Encryption, and the encryption status is "Encrypted."

The type of encryption on a client computer affects how some policies are handled:

- When drives are hardware-encrypted, the policy options on the Drive Encryption - Encryption policy, such as the encryption strength or inclusion of unused disk space, are not applicable.
- If a drive is software encrypted when the Drive Encryption - Self-Encrypting Drives policy is deployed, the policy is ignored on the client computer.
To move an Opal v2 compliant drive from software encryption to hardware encryption, after you upgrade to Symantec Endpoint Encryption to 11.1.2:

1 Prerequisites:
   ■ Make sure that the drive appears on the whitelist of supported Opal drives.
   ■ If the drive is a Microsoft eDrive support - Opal v2 compliant drive, verify the drive’s partitions. Make sure that:
      ■ The default partitions were created during a default Microsoft Windows installation, and
      ■ When multiple partitions exist, the number of ranges is properly mapped to the number of partitions.

2 Decrypt the drive using Symantec Endpoint Encryption. To issue decrypt commands, do the following:
   ■ From the Management Server, use the Server Commands snap-in, or
   ■ From the client computer, ask a client administrator to use either the Drive Encryption Administrator Command Line or the Client Administrator Console.

3 Configure and deploy the Drive Encryption - Self-Encrypting Drives install-time, GPO, or native policy, with the Use hardware encryption for compatible Opal-compliant drives option enabled.

4 Re-issue an encrypt command from Symantec Endpoint Encryption. To issue encrypt commands, do the following:
   ■ From the Management Server, use the Server Commands snap-in, or
   ■ From the client computer, ask a client administrator to use either the Drive Encryption Administrator Command Line or the Client Administrator Console.

The encrypt command recognizes the Opal v2 compliant drive and attempts to manage and secure the drive. If a drive is not provisioned in Single User Mode, Drive Encryption provisions it in Global Range Mode.

**Updating the existing GPO or native BitLocker Client policies post upgrade**

After you upgrade the Symantec Endpoint Encryption Management Server and Manager Console to version 11.1.2, as a best practice, revisit the BitLocker client policies for encryption (Encryption and Authentication policy) and client lockout (Client Monitor policy). Note that the BitLocker client GPO and native policies are also now available as an install-time policy in version 11.1.2.
Upgrading the Autologon Utility

When you upgrade clients to Symantec Endpoint Encryption 11.1.2, the Autologon Utility is uninstalled. To enable the Autologon feature again, you must create a new Autologon Utility installation package and deploy it on the client computer. When the upgrade is complete, restart the client computer.

Installing additional client features after upgrading

Optionally, after you complete the upgrade to version 11.1.2, you can install additional features that were not previously enabled. For example, after you finish upgrading Drive Encryption, you can install Removable Media Encryption on the client computers.

To install additional features, you must create a new Symantec Endpoint Encryption Client installation package that has the new feature enabled. Be aware that some features cannot co-exist with other features.

See “About enabling features in the Symantec Endpoint Encryption Client installation package” on page 93.

When you are ready, deploy the new Symantec Endpoint Encryption Client installation package using the following command:

```
MSIEXEC /i "[path]\msifile" REINSTALLMODE=vemus ADDLOCAL=ALL /l*v "[logpath]\logfile"
```

Where [path]\msifile represents the path and name of the MSI file, and [logpath]\logfile represents the path and name of the output log file.

When the installation is complete, restart the client computer.

---

**Note:** When you upgrade the Symantec Endpoint Encryption Client, you must also upgrade any additional features that are installed, such as the Autologon Utility and the Windows Password Reset Utility.

---

Using Group Policy Objects when upgrading Microsoft Windows clients

While upgrading clients to Symantec Endpoint Encryption 11.1.2, you can use a GPO to distribute the Symantec Endpoint Encryption Client installation package to the computers in your organization.

When you deploy Symantec Endpoint Encryption Client 11.1.2 on a Microsoft Windows computer, the installer performs one of the following actions:
If you upgrade from Symantec Endpoint Encryption 11.x, the existing features are upgraded, and additional features are installed if they are enabled in the MSI file.

If you upgrade from Symantec Endpoint Encryption 8.2.1, the Framework, Full Disk and Removable Storage clients are uninstalled. Symantec Endpoint Encryption Client is installed without decrypting the disk.

If you upgrade from Symantec Encryption Desktop 10.3.2 MP4, MP9, MP10, or MP11, only the Symantec Drive Encryption feature is disabled. Symantec Endpoint Encryption Client is installed without decrypting the disk, and no other Symantec Encryption Desktop features are disabled. If required, you can uninstall Symantec Encryption Desktop later.

**Note:** If the currently installed version of the Symantec Endpoint Encryption client software was deployed using a GPO, before you upgrade to version 11.1.2, update the GPO to remove the original MSI file. Make sure that you do not select the option to uninstall the client software when you update the GPO.

Tailor the following procedures to suit the requirements of your organization.

**Creating Symantec Endpoint Encryption Client installers for distribution**

**To create Symantec Endpoint Encryption client installers for distribution**

- Create the MSI file for Symantec Endpoint Encryption Client. Choose the 32-bit or 64-bit version, as appropriate for the version of Microsoft Windows installed on your client computers.

**Note:** If you upgrade a client using a Symantec Endpoint Encryption Client installation package that was created using a different Symantec Endpoint Encryption Management Server, the Help Desk Recovery feature stops working as the client computer does not exist in the new server’s database. After the upgrade is complete, ensure that the client checks in with Symantec Endpoint Encryption Management Server. Then, disable and re-enable the Help Desk Recovery feature through the policy settings.

For more information about creating the Symantec Endpoint Encryption Client installation package, see the *Creating Symantec Endpoint Encryption client installers* chapter available in the *Symantec Endpoint Encryption Management Server Online Help*. 
See “Creating a Symantec Endpoint Encryption Client installation package” on page 72.

Creating an Active Directory distribution point

To create a distribution point on your Active Directory forest or domain

1. Save the created MSI file that you want to deploy using a GPO in a folder that is in a shared network location. For example, the location can be the domain controller's SYSVOL folder. The created folder is the distribution point on your Active Directory forest or domain.

2. Set the folder properties to enable users to have read and execute permissions. For example, you can avoid access permission issues during deployment if you set the security property of the shared folder to Everyone.

---

**Caution:** Carefully review your procedures on your network and follow the rights assignment policies of your organization. Reset the security property of the shared folder immediately when you finish deployment.

Creating an upgrade script file

Create a startup script to run the following command on the client computers that you want to upgrade to Symantec Endpoint Encryption 11.1.2:

```
MSIEXE /i "[path]\msifile" /norestart CONDITION_NOUI=1 /l*v
"[logpath]\logfile"
```

Where `[path]\msifile` represents the share path and name of the MSI file, and `[logpath]\logfile` represents the path and name of the output log file.

---

**Note:** Refer to the sample upgrade script that is provided in the Symantec Knowledge Base article http://www.symantec.com/docs/HOWTO124269.

Creating GPOs to deploy the upgrade script

To create Group Policy Objects and deploy the upgrade script

---

**Note:** If User Account Control (UAC) is enabled on a client computer, you must enable the **Always install with elevated privileges** group policy setting under **Computer Configuration** and **User Configuration** in the **Group Policy Management Editor**.
2. In the left pane, expand Group Policy Management.
3. Right-click Group Policy Objects and click New.
4. In the New GPO window, type a GPO title in the Name box and click OK to save the new policy.

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

5. Right-click the created GPO, and select Edit.
6. In the left pane of the Group Policy Management Editor, navigate to Computer Configuration > Policies > Windows settings > Scripts (Startup/Shutdown).
7. In the right pane, double-click Startup.
9. In the Add a script dialog box, click Browse.
10. Using the navigation windows to select the script file, and then click Open.
11. To submit the script file, click OK.
12. To close the Startup Properties dialog box, click OK.
13. Close the Group Policy Management Editor.

**Installing the client installer GPOs**

After you finish configuring the GPO, restart the client computers to begin the upgrade.

**Note:** When you upgrade the Symantec Endpoint Encryption Client, you must also upgrade any additional features that are installed, such as the Autologon Utility and the Windows Password Reset Utility.

---

**Upgrading Symantec Endpoint Encryption for FileVault clients**

Before you upgrade Symantec Endpoint Encryption for FileVault to version 11.1.2, ensure that the disk is either completely encrypted or decrypted. If encryption or decryption is in progress, wait until the disk is completely encrypted or decrypted.
To upgrade Symantec Endpoint Encryption for FileVault manually


To upgrade Symantec Endpoint Encryption for FileVault using the command line

1. Launch the Terminal application.
2. In the Terminal window, enter the following command:
   
   ```
   sudo installer -package [filepath] -target /
   ```

   where, `[filepath]` represents the location and name of the Symantec Endpoint Encryption for FileVault installation package file.
Uninstalling the Symantec Endpoint Encryption client software

This chapter includes the following topics:

■ About uninstalling the Symantec Endpoint Encryption client

■ Uninstalling the Symantec Endpoint Encryption client software using the Control Panel

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

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

■ Uninstalling the Symantec Endpoint Encryption client software using the command line

■ Uninstalling Symantec Endpoint Encryption for FileVault

About uninstalling the Symantec Endpoint Encryption client

When you uninstall Symantec Endpoint Encryption from client computers, you can either uninstall specific features separately or uninstall all of the features together.
**Note:** While uninstalling features separately, you can specify only Drive Encryption, Symantec Endpoint Encryption for BitLocker, and Removable Media Encryption. The Management Agent is removed automatically when there are no other features left to uninstall.

You can uninstall Symantec Endpoint Encryption in the following ways:

- Using a third-party tool to execute an uninstallation script on the client computers
- Using a GPO
- Using the Control Panel in Microsoft Windows
- Using the Command Prompt

**Note:** The uninstallation of specific features is possible only from the Command Prompt or by using a third-party tool with an uninstallation script.

**Prerequisites**

Before you uninstall the Drive Encryption feature:

- Make sure that all fixed disks are fully decrypted.
- (Optional) Make sure that the Autologon feature is uninstalled.
- (Optional) Make sure that the Windows Password Reset Utility is uninstalled.

Before you uninstall the Symantec Endpoint Encryption for BitLocker feature:

- On encrypted systems, ensure that the users back up their BitLocker Recovery Key for recovery. Symantec Endpoint Encryption Management Server does not store the BitLocker Recovery Key after the Symantec Endpoint Encryption for BitLocker client is uninstalled from the system. Encrypted systems can be uninstalled without being decrypted.

**Note:** If Symantec Endpoint Encryption manages this computer, you should manually delete it from the Management Console after you uninstall.

See “About uninstalling the Symantec Endpoint Encryption client with a third-party tool” on page 280.

See “About uninstalling the Symantec Endpoint Encryption client software using Group Policy Objects” on page 281.

See “Uninstalling the Symantec Endpoint Encryption client software using the Control Panel” on page 279.
See “Uninstalling the Symantec Endpoint Encryption client software using the command line” on page 284.

Uninstalling the Symantec Endpoint Encryption client software using the Control Panel

You can uninstall the Symantec Endpoint Encryption client software from a Microsoft Windows computer by using the Windows Add/Remove Programs utility. However, if the client software was installed using a Group Policy Object, it can only be uninstalled through that same GPO.

Perform the following procedure to uninstall the Symantec Endpoint Encryption client software using the Add/Remove Programs utility in the Control Panel.

**Note:** This uninstallation method removes all of the Symantec Endpoint Encryption features from client computers.

To uninstall the Symantec Endpoint Encryption client software manually:

1. Log on to the client computer using an administrator account or another account with sufficient privileges to uninstall software.

2. To access the Control Panel, do one of the following:
   - For Microsoft Windows 7, click **Start > Control Panel**.
   - For Microsoft Windows 8.x, access the **Start** screen, and type **Control Panel**. In the **Apps** search results, click the **Control Panel** icon.
   - For Microsoft Windows 10, in the **Search the web and Windows** search bar, type **Control Panel**. In the search results menu, click the **Control Panel** icon.

3. Do one of the following:
   - In the **Category** view of the Control Panel, under **Programs**, click **Uninstall a program**.
   - Click **Programs and Features**.

4. In the **Programs and Features** window, select Symantec Endpoint Encryption Client.

5. Click **Uninstall**.

6. If prompted to confirm, click **Yes**.
7 (Optional) If Symantec Endpoint Encryption Autologon Client and Windows Password Reset Utility are also listed in the Programs and Features window, uninstall them the same way.

8 After all of the clients are uninstalled, restart the computer when prompted.

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

You can uninstall the Symantec Endpoint Encryption Client package using any third-party deployment tool that supports the MSI format.

**Note:** Make sure that the client computers fulfill the uninstallation prerequisites before you attempt to uninstall Symantec Endpoint Encryption Client.

For large-scale deployments, you can use the command line as a basis for scripted uninstalls.

For example, you can create a batch file to invoke the Windows Installer (msiexec.exe). This batch file can contain one or more of the following commands:

- To uninstall the Drive Encryption feature:
  ```cmd
  msiexec /i "[path]\msifile" REMOVE="DE" /l*v "[logpath]\logfile"
  ```

- To uninstall the Symantec Endpoint Encryption for BitLocker feature:
  ```cmd
  msiexec /i "[path]\msifile" REMOVE="BL" /l*v "[logpath]\logfile"
  ```

- To uninstall the Removable Media Encryption feature:
  ```cmd
  msiexec /i "[path]\msifile" REMOVE="RME" /l*v "[logpath]\logfile"
  ```

- To uninstall the all of the Symantec Endpoint Encryption features together:
  ```cmd
  msiexec /x "[path]\msifile" /l*v "[logpath]\logfile"
  ```

Where [path]\msifile represents the path and name of the MSI file, and [logpath]\logfile represents the path and name of the output log file.

**Note:** If you want to uninstall Symantec Endpoint Encryption Client from both 32-bit and 64-bit computers, make sure that the commands specify the appropriate MSI files.
About uninstalling the Symantec Endpoint Encryption client software using Group Policy Objects

If you used a Group Policy Object to deploy Symantec Endpoint Encryption clients, you must use the same GPO to uninstall them.

**Note:** You should never manually uninstall GPO-deployed client packages either manually or from the command line.

The uninstallation process consists of the following steps:

1. If you used a GPO to deploy the Drive Encryption feature, issue a server command to decrypt all of the fixed drives on all of the targeted computers.

2. If you used a GPO to deploy the Removable Media Encryption feature, manually decrypt all of the files on the removable drives that do not contain the Removable Media Access Utility.

3. Uninstall the desired features, or all of them.

Depending upon the way in which you deployed Symantec Endpoint Encryption 11.1.2, there are two ways to uninstall the clients using GPOs:

- Completely uninstall the Symantec Endpoint Encryption Client package from all of the client computers by removing the MSI file from the GPO. This method is available only if you installed Symantec Endpoint Encryption 11.1.2 directly, for example, you did not use a GPO to upgrade to version 11.1.2.

- Deploy an uninstallation script to remove the desired features, or all of them. This method is available only if you used a GPO to upgrade to Symantec Endpoint Encryption 11.1.2 from an earlier product.

As a best practice, you should set the appropriate Microsoft Windows policies to prevent users from manually removing the client packages.

**Note:** Uninstallation fails if all drives are not fully decrypted.

See “Uninstalling the Symantec Endpoint Encryption Client installation package using Group Policy Objects” on page 282.

See “Deploying uninstallation scripts using Group Policy Objects” on page 283.
Uninstalling the Symantec Endpoint Encryption Client installation package using Group Policy Objects

Uninstall the GPO-managed client installation package when you want to uninstall all of the Symantec Endpoint Encryption features at the same time. You can use this uninstallation method only if you used a GPO to install Symantec Endpoint Encryption 11.1.2 directly, and have not upgraded from an earlier product.

Note: Make sure that the client computers fulfill the uninstallation prerequisites before you attempt to uninstall Symantec Endpoint Encryption Client. See “About uninstalling the Symantec Endpoint Encryption client” on page 277.

To uninstall the Symantec Endpoint Encryption Client installation package using GPOs

1. In the navigation pane of the Management Console, expand the Group Policy Management snap-in.
2. Expand the domain in which you want to uninstall the client software.
4. Right-click the GPO that you used to deploy the client software, and select Edit.
5. In the Group Policy Management Editor window, expand Computer Configuration.
6. Expand Policies > Software Settings
7. Right-click Software installation, and select Properties.
8. In the Software installation Properties dialog box, click the Advanced tab.
9. To configure the GPO to uninstall the unmanaged software packages from the subscribed computers, check Uninstall the applications when they fall out of the scope of management.
10. Click OK to close the dialog box.
11. In the navigation pane of the Group Policy Management Editor window, click Software installation.

   The right pane of the window displays a list of the software packages that were deployed using this GPO.
12. Right-click the software package that you want to uninstall from all of the computers in the domain, and select Remove.
In the Remove Software dialog box, check **Immediately uninstall the software from users and computers** and click **OK**.

Close the **Group Policy Management Editor** window.

### Deploying uninstallation scripts using Group Policy Objects

Deploying an uninstallation script enables you to uninstall specific Symantec Endpoint Encryption features from the client computers. Alternatively, you can also use an uninstallation script to completely uninstall Symantec Endpoint Encryption from the client computers.

**Note:** You can use this uninstallation method only if you used a GPO to upgrade to Symantec Endpoint Encryption 11.1.2 from an earlier product.

### Before you begin

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

See “About uninstalling the Symantec Endpoint Encryption client” on page 277.

### Creating an uninstallation script file

Create a script file that includes one or more of the following commands:

- To uninstall the Drive Encryption feature:
  
  ```
  MSIEXEC /i "[path]\msifile" REMOVE=DE /l*v "[logpath]\logfile"
  ```

- To uninstall the Symantec Endpoint Encryption for BitLocker feature:
  
  ```
  MSIEXEC /i "[path]\msifile" REMOVE=BL /l*v "[logpath]\logfile"
  ```

- To uninstall the Removable Media Encryption feature:
  
  ```
  MSIEXEC /i "[path]\msifile" REMOVE=RME /l*v "[logpath]\logfile"
  ```

- To uninstall all of the Symantec Endpoint Encryption features together:
  
  ```
  MSIEXEC /x "[path]\msifile" /l*v "[logpath]\logfile"
  ```

Where `[path]\msifile` represents the share path and name of the MSI file, and `[logpath]\logfile` represents the path and name of the output log file.

### Configuring GPOs to deploy the uninstallation script

**Note:** If your network includes both 32-bit and 64-bit systems, make sure that you update all of the relevant GPOs.
To configure GPOs to deploy the uninstallation script

2. In the left pane, expand Group Policy Management and navigate to the GPO that you previously used to upgrade the Symantec Endpoint Encryption clients.
3. Right-click the GPO and click Edit.
4. In the left pane of the Group Policy Management Editor, navigate to Computer Configuration > Policies > Windows settings > Scripts (Startup/Shutdown).
5. In the right pane, double-click Startup.
7. In the Add a script dialog box, click Browse.
8. Using the navigation windows to select the uninstallation file, and then click Open.
9. To submit the script file, click OK.
10. In the Startup Properties dialog box, select the upgrade script that you previously used to upgrade the Symantec Endpoint Encryption clients, and click Remove.
11. To close the Startup Properties dialog box, click OK.
12. Close the Group Policy Management Editor.

Deploying the uninstallation script

After you finish configuring the GPO, restart the client computers to begin the uninstallation.

Uninstalling the Symantec Endpoint Encryption client software using the command line

Client Administrators can use the command prompt to uninstall one or more Symantec Endpoint Encryption features from a single computer. You can also uninstall the Autologon Utility. The results of the uninstallation are saved in a log file that you specify.

Note: Make sure that the client computers fulfill the uninstallation prerequisites before you attempt to uninstall Symantec Endpoint Encryption Client. See “About uninstalling the Symantec Endpoint Encryption client” on page 277.
If you are prompted to restart the computer after uninstalling one or more client software, accept the prompt. When Microsoft Windows starts, return to the command prompt and enter the remaining commands to uninstall the remaining software.

Note: To perform a silent installation, append the commands in the following procedure with the \texttt{CONDITION\_NOUI=1} parameter.

To uninstall Symantec Endpoint Encryption client software using the command line:

1. Click \textit{Start} > \textit{Run}.
2. In the \textit{Run} dialog box, type \texttt{cmd}.
3. To open the command prompt, click \textit{OK}.
4. (Optional) To uninstall the Autologon Utility when the Autologon feature is enabled permanently, enter one of the following commands:
   - For 32-bit systems:
     \begin{verbatim}
     msiexec -x "[Path]\Autologon Infinite DD MMM YYYY.msi" /qn /live LogFilePath
     \end{verbatim}
   - For 64-bit systems:
     \begin{verbatim}
     msiexec -x "[Path]\Autologon Infinite_x64 DD MMM YYYY.msi" /qn /live LogFilePath
     \end{verbatim}
5. (Optional) To uninstall the Autologon Utility when the Autologon feature is enabled by a client administrator, enter one of the following commands:
   - For 32-bit systems:
     \begin{verbatim}
     msiexec -x "[Path]\Autologon NoAutologon.msi" /qn /live LogFilePath
     \end{verbatim}
   - For 64-bit systems:
     \begin{verbatim}
     msiexec -x "[Path]\Autologon NoAutologon_x64.msi" /qn /live LogFilePath
     \end{verbatim}
6. (Optional) To uninstall the Drive Encryption feature, enter one the following commands:
   - For 32-bit systems:
     \begin{verbatim}
     msiexec -i "[Path]\SEE Client.msi" REMOVE=DE /l+v LogFilePath
     \end{verbatim}
   - For 64-bit systems:
     \begin{verbatim}
     msiexec -i "[Path]\SEE Client x64.msi" REMOVE=DE /l+v LogFilePath
     \end{verbatim}
7 (Optional) To uninstall the Removable Media Encryption feature, enter one the following commands:

- For 32-bit systems:
  msiexec -i "[Path]\SEE Client.msi" REMOVE=RME /l*v LogFilePath

- For 64-bit systems:
  msiexec -i "[Path]\SEE Client x64.msi" REMOVE=RME /l*v LogFilePath

8 (Optional) To uninstall the Symantec Endpoint Encryption for BitLocker feature, enter one the following commands:

- For 32-bit systems:
  msiexec -i "[Path]\SEE Client.msi" REMOVE=BL /l*v LogFilePath

- For 64-bit systems:
  msiexec -i "[Path]\SEE Client x64.msi" REMOVE=BL /l*v LogFilePath

9 (Optional) To uninstall the all of the Symantec Endpoint Encryption Client features, enter one the following commands:

- For 32-bit systems:
  msiexec -x "[Path]\SEE Client.msi" /l*v LogFilePath

- For 64-bit systems:
  msiexec -x "[Path]\SEE Client x64.msi" /l*v LogFilePath

**Uninstalling Symantec Endpoint Encryption for FileVault**

Perform the following procedure to uninstall Symantec Endpoint Encryption for FileVault from a Macintosh computer. You do not have to decrypt the disk before uninstalling Symantec Endpoint Encryption for FileVault.

**Note:** Make sure that you have administrator privileges.
To uninstall Symantec Endpoint Encryption for FileVault

1. Launch the Terminal application.

2. Using Terminal, navigate to the `/Library/Application Support/Symantec Endpoint Encryption/` directory.

3. Type the following command:
   
   `sudo ./uninstall`
Multimedia file types excluded in Symantec Endpoint Encryption

This appendix includes the following topics:

■ Audio file types excluded
■ Video file types excluded
■ Image file types excluded

Audio file types excluded

Table A-1

<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>File Extension</td>
<td>File Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------------</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>RIFF</td>
<td>Resource Interchange File Format</td>
<td>Standard MIDI data, RIFF (little/big-endian) data MIDI</td>
</tr>
</tbody>
</table>
Table A-1 (continued)

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 file types excluded

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</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>File Extension</td>
<td>File Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>F4V</td>
<td>Adobe Flash container (ISO/IEC 14496-12)</td>
<td>Macromedia Flash Data/Video</td>
</tr>
<tr>
<td>FLC</td>
<td>Animation file created by Autodesk</td>
<td>FLIC animation</td>
</tr>
<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 AVC, iTunes AVC-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 AVC, iTunes AVC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>File Extension</td>
<td>File Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------------</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 AVC, iTunes AVC-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 AVC, iTunes AVC-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 AVC, iTunes AVC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<tr>
<td>File Extension</td>
<td>File Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------------</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 AVC, iTunes AVC-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 AVC, iTunes AVC-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 AVC, iTunes AVC-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>
</tbody>
</table>
Table A-2  (continued)

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 AVC, iTunes AVC-LC, bookmarked, AES encrypted), MPEG sequence, MPEG-4 LOAS/LO-EP audio stream, transport stream data</td>
</tr>
<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 file types excluded

Table A-3

<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>
</tbody>
</table>
### Table A-3 (continued)

<table>
<thead>
<tr>
<th>File Extension</th>
<th>File Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
<tr>
<td>PSD</td>
<td>raster image containing Photoshop-specific elements</td>
<td>Adobe photoshop images</td>
</tr>
<tr>
<td>File Extension</td>
<td>File Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------------</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>
A

Active Directory
all drives on all computers in a group
  decrypting using server-based commands 186
  encrypting using server-based commands 186
  synchronization, viewing 207
Active Directory computers
  about 166
  status, viewing 210
Active Directory distribution point
  creating 102, 272
Active Directory policies
  about 38
  deployment, verifying 243
Active Directory policies and native policies
  comparing 39
Active Directory policy options 52
admin logs
  about 207
  viewing 207
administrative policies
  about 37
  accessing 111
  by task, identifying 54
  configuring 109
  machine catalogs 161
  types 38
  virtual desktop clients 161
AES encryption strength
  128-bit, 256-bit 130
  setting 130
all drives on a computer
  decrypting using server-based commands 187
  encrypting using server-based commands 187
authentication method
  password, configuring 122
  registered users 122
  token, configuring 122

Autologon
  bypassing authentication 177
  installing 179
  MSI files, creating 178
  pre-requisite, creating 178
  precaution 177

B
backward compatibility
  see Removable Media Encryption policy options, encryption format 135
best practices
  data recovery 258
  recovery certificate, using 143
BitLocker Client
  policy options 40
BitLocker Client policy options
  Authentication, including 150
  client monitor, configuring 151
  Encryption, including 150
  process overview 150

C
CD/DVD Burner
  moving files between 11.x and 8.2.1
  computers 138
  Removable Media Encryption Burner Application
    description 86
client
  about uninstalling with GPO 281
  deploying uninstallation scripts with GPO 283
  uninstalling 277
  uninstalling manually 279
  uninstalling the installation package with GPO 282
  uninstalling using the command line 284
  uninstalling using the Control Panel 279
  uninstalling with third-party tools 280
client administrators
  creating CSV files 120
  importing and exporting 117, 119
client administrators  (continued)
load from MSI 121
privileges 119
client computers
decrypted drives, viewing 215
expired certificates, viewing 217
non-Drive Encryption, viewing 220
non-Removable Media Encryption, viewing 222
non-reporting 225
Opal v2 compliant drive, viewing 240
policy details, viewing 228
specified users, viewing 219
client installation package
about 69
client installer deployment
command line, using 106
Group Policy Object, using 102
third-party tool, using 101
client installers
about 69
Active Directory deployment, using 102
command line, deploying 106
command line, upgrading 268
command line, using 106
Group Policy Object, deploying 102
client software
installing manually 104
client upgrades
Active Directory deployment, using 272
command line, using 268
Group Policy Object, using 272
computer reports
Computers BitLocker Status 232
computers with decrypted drives 215
computers with expired certificates 217
Computers with Hardware Encrypted Drives 240
customers with specified users 219
computers without Drive Encryption 220
computers without Removable Media Encryption 222
decrypt drive 241
encrypt drive 241
Mac Computers FileVault Status 230
non-reporting computers, viewing 225
Removable Media Encryption details 228
computer status report
viewing 210

D
data recovery
Macintosh encrypted disk 259
database maintenance
about 34
disaster recovery
about 19
data, backing up 21
database, backing up 20
options 22
Windows PE, using 22
Drive Encryption
install-time policies, configuring 76
installation settings, configuring 76
policy options 40
Drive Encryption login screen
xpm files, using 128
Drive Encryption policy options
AES encryption strength, setting 130
authentication method, configuring 122
client administrators, adding 117
client administrators, deleting 121
client administrators, editing 117
client administrators, privileges 119
client monitor, configuring 131
double-write sector, configuring 130
encryption of unused disk space, setting 130
Help Desk Recovery, configuring 132
login screen, customizing 126
logon message, customizing 126
One-Time Password, configuring 132
Opal v2 compliant drives 132
process overview 115
remote decryption, configuring 134
Self-Encrypting Drives, configuring 132
Self-Recovery, configuring 125
single sign-on, configuring 125
startup image, customizing 126
user logon history, configuring 130
Windows Password Reset, configuring 133
Drive Encryption Self-Recovery
configuring 125
minimum answer length 125
predefined questions 125
supported character set 125
Drive Encryption single sign-on
enabling, disabling 125
Drive Encryption startup (splash) screen
xpm files, using 128
E

event logs
  about 209
  viewing 209
expired certificates
  report 217

F

file recovery
  recovery certificate 142
file types
  audio, excluding 139
  image, excluding 139
  video, excluding 139

G

GPO
  about uninstalling clients 281
  deploying uninstallation scripts 283
  uninstalling installation packages 282
GPOs
  creating 154
  deploying 167
  editing 154
  Group Policy Report 168
  order of precedence 168
  overview 154
  overview, deploying 166
  updates, forcing 167

H

Help Desk Recovery
  about 247
  bitlocker recovery key 247
  BitLocker Recovery Key, providing 257
  challenge key 247
  institutional recovery key 247
  offline 247
  online 247
  personal recovery key 247
  Personal Recovery Key, providing 256
  providing 250
  response key 247
  response key, providing 250

I

install-time policies
  about 38
  restoring 154
install-time policy
  options 52

M

Mac FileVault Client
  policy options 40
Mac FileVault Client policy options
  communication 149
  Institutional Recovery Key, including 148
  introduction 147
  process overview 146
managed computer groups
  about 169
  computers, deleting 172
  computers, moving 171
  creating 170
Management Agent
  install-time policies, configuring 73
  installation settings, configuring 73
  policy options 40
Management Agent installation settings wizards
  about 70
Management Agent Password Authentication policy
  password authentication, configuring 113
Management Agent policy options
  communication, configuring 115
  password authentication, configuring 113
  process overview 112
Management Password
  about 17
  changing 18

N

native policies
  about 38
  assigning 175
  assigning to Novell eDirectory computers 175
  assigning, overview 175
  creating 158
  editing 158
  overview 158
  overview, deploying 168
  updates, forcing 176
Policy creation about 153
Policy management about 153
Policy types accessing 111
Portability
Removable Media Access Utility, selecting 144
Self-Decrypting Archive, selecting 144
Preboot authentication bypassing 177
xpm files 128
Reports
Active Directory forests synchronization status 207
Active Directory synchronization, viewing 207
Admin log, viewing 207
Client events log, viewing 209
Columns, about 199
Computer status 210
Customizing 198
Encrypted endpoints percentage 228
Endpoint encryption status, viewing 212
Exempted device, viewing 224
Exporting 197
Group policy, deploying 243
Novell eDirectory synchronization status 227
RSoP 243
Server commands 197
Server commands, viewing 241
Roles, server. See Server Roles
Server Roles
Configuring 31
Defining 27
Disabling 33
Editing 33
Overview 27
Removing 33
Server-based commands
about 183
Removable Media Encryption policy options (continued)
Automatic encryption, configuring 135
default password, configuring 140
device session password, configuring 140
device, excluding 139
Encryption format, backward compatibility 135
Encryption format, configuring 135
Encryption format, for Burner Application 135
Encryption method, configuring 140
Expired certificates, configuring 145
File type, excluding 139
On-demand encryption, configuring 135
Password aging, password history 140
Portability, configuring 144
Process overview 134
Recovery certificate, configuring 142
Session passwords, configuring 140
Workgroup key, configuring 145
Removable Media Encryption policy options
access, configuring 135
Removable Media Encryption encryption method
Certificate, selecting 140
Password, selecting 140
Removable Media Encryption policy options
Access, configuring 135
Opal drives
See Drive Encryption policy options,
Self-Encrypting Drives, configuring 132
Opal v2 compliant drives
Upgrading 270
One-Time Password
Providing 252
One or more drives on a computer
Decrypting using server-based commands 187
Encrypting using server-based commands 187
Index
server-based commands (continued)
execution, forcing 188
fixed disk drives, decrypting 186
fixed disk drives, encrypting 186
pending command, canceling 188
process overview 185
Symantec Endpoint Encryption
about 15
clients, installing 261
database access, regaining 24
disaster recovery 22
key features 15
policy options 40
recovery sequence 23
user registration, silent 123
Symantec Endpoint Encryption Client
features, modifying 93
install-time policies, configuring 72
installation package
features 93
installation package, creating 72
installation settings, configuring 72
installing manually 104
Symantec Endpoint Encryption for BitLocker
install-time policies, configuring 84
installation settings, configuring 84
Symantec Endpoint Encryption for FileVault
install-time policies, configuring 97
installation package, creating 97
installing manually 104
uninstalling 286
Symantec Endpoint Encryption logs
about 25
Symantec Endpoint Encryption managed computers
group
all drives on all computers in a group
decrypting using server-based
commands 186
encrypting using server-based
commands 186
Symantec Endpoint Encryption Management Server
administrators 16
Symantec Endpoint Encryption policies
conflicts and precedence 176
prerequisites 16
Symantec Endpoint Encryption policy options
about 109
accessing 111
configuring 109
Symantec Endpoint Encryption reports
about 195
additional features 197
columns, adding 198
custom reports, creating 245
custom reports, editing 246
exempted removable media 224
extended columns 199
types 196
Symantec Endpoint Encryption users
registering 123

U
uninstalling
about uninstalling the client with GPO 281
client 277
command line, using 284
Control Panel 279
deploying uninstallation scripts with GPO 283
Mac OS X 286
Symantec Endpoint Encryption for FileVault 286
uninstalling the client manually 279
uninstalling the client with third-party tools 280
uninstalling the installation package with
GPO 282
upgrading
command line, using 268
user logon history
domain, viewing 130
user name, viewing 130
user registration
about 123

W
Whole Disk Recovery Token
providing 254
Windows Password Reset Utility
installing 105