The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.


Legal Notice

Copyright (c) 2013 Symantec Corporation. All rights reserved.
Symantec, the Symantec Logo, the Checkmark Logo, PGP, Pretty Good Privacy, and the PGP logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

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. 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
Symantec Home Page (http://www.symantec.com)
Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1
# Contents

## Overview

<table>
<thead>
<tr>
<th>Who Should Read This Guide</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Terms</td>
<td>4</td>
</tr>
<tr>
<td>Other Relevant Resources</td>
<td>4</td>
</tr>
<tr>
<td>Technical Support</td>
<td>5</td>
</tr>
<tr>
<td>Contacting Technical Support</td>
<td>6</td>
</tr>
<tr>
<td>Licensing and registration</td>
<td>6</td>
</tr>
<tr>
<td>Customer service</td>
<td>6</td>
</tr>
<tr>
<td>Support agreement resources</td>
<td>7</td>
</tr>
</tbody>
</table>

## Understanding Symantec Drive Encryption

| About Symantec Drive Encryption | 9 |
| Components of a Typical Symantec Drive Encryption Deployment | 10 |
| How Does Symantec Drive Encryption Work? | 10 |
| About Symantec Encryption Management Server | 11 |

## Major Steps

<table>
<thead>
<tr>
<th>Preparation</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placing the Symantec Encryption Management Server in your Network</td>
<td>15</td>
</tr>
<tr>
<td>Adding the Symantec Encryption Management Server to your Network</td>
<td>16</td>
</tr>
<tr>
<td>Deployment Options</td>
<td>16</td>
</tr>
<tr>
<td>Configuring your Firewall</td>
<td>17</td>
</tr>
<tr>
<td>Understanding Enrollment</td>
<td>18</td>
</tr>
<tr>
<td>Understanding the Two Enrollment Paths</td>
<td>18</td>
</tr>
<tr>
<td>Understanding the LDAP Directory Synchronization Feature</td>
<td>19</td>
</tr>
<tr>
<td>Understanding Policies</td>
<td>19</td>
</tr>
<tr>
<td>Preparing End-User Systems</td>
<td>20</td>
</tr>
</tbody>
</table>

## Installation and Configuration

| Before You Install | 21 |
| Installing the Server Software | 21 |

## Configuring the Symantec Encryption Management Server

| Removing Unneeded Services | 23 |
| Setting Up Administrators | 24 |
| Establishing Backups | 24 |
| Securing your Symantec Encryption Management Server | 25 |
| Configuring Policies | 25 |
| Configuring the LDAP Directory Synchronization Feature | 26 |
| Configuring Enrollment | 27 |
| Email Enrollment | 27 |
LDAP Directory Synchronization Enrollment

Establishing Symantec Drive Encryption Client Settings

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td>29</td>
</tr>
<tr>
<td>Key Settings</td>
<td>29</td>
</tr>
<tr>
<td>Key Generation Settings</td>
<td>30</td>
</tr>
<tr>
<td>Key Mode Settings</td>
<td>30</td>
</tr>
<tr>
<td>Certificates Settings</td>
<td>31</td>
</tr>
<tr>
<td>Options Settings</td>
<td>31</td>
</tr>
<tr>
<td>Symantec Encryption Desktop Settings</td>
<td>32</td>
</tr>
<tr>
<td>General Tab</td>
<td>32</td>
</tr>
<tr>
<td>Messaging &amp; Keys Tab</td>
<td>36</td>
</tr>
<tr>
<td>Zip &amp; Shredder Tab</td>
<td>38</td>
</tr>
<tr>
<td>File Share Tab</td>
<td>38</td>
</tr>
<tr>
<td>Drive Encryption Tab</td>
<td>39</td>
</tr>
<tr>
<td>Licensing Settings</td>
<td>44</td>
</tr>
</tbody>
</table>

Creating the Symantec Drive Encryption Client Installer

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating an Installer with Auto-Detect Policy</td>
<td>45</td>
</tr>
<tr>
<td>Creating an Installer with Preset Policy</td>
<td>46</td>
</tr>
<tr>
<td>Creating an Installer with No Policy Settings</td>
<td>47</td>
</tr>
</tbody>
</table>

Controlling Symantec Drive Encryption Components

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing the Symantec Drive Encryption Client Installer</td>
<td>51</td>
</tr>
</tbody>
</table>

Deploying the Symantec Drive Encryption Client Installer

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assisting Your Symantec Drive Encryption Users</td>
<td>55</td>
</tr>
</tbody>
</table>

The End-User Experience

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>During the Installation Process</td>
<td>57</td>
</tr>
<tr>
<td>During Symantec Drive Encryption Setup</td>
<td>58</td>
</tr>
<tr>
<td>During Normal Usage</td>
<td>58</td>
</tr>
</tbody>
</table>
Overview

This Guide describes how to create, deploy, and manage the Symantec Drive Encryption product in an enterprise environment, using the Symantec Encryption Management Server product as the management console.

Some of the information in this Guide also applies to deploying any Symantec Encryption Desktop client product.

In This Chapter

Who Should Read This Guide ................................................................................................................. 3
Important Terms .......................................................................................................................... 4
Other Relevant Resources .................................................................................................................. 4
Technical Support .......................................................................................................................... 5

Who Should Read This Guide

This Guide assumes you are an IT or support professional who will be performing one or more of the following deployment tasks:

- Setting up and configuring the Symantec Encryption Management Server as the management console.
- Understanding and configuring Symantec Drive Encryption client options.
- Creating, testing, and distributing the Symantec Drive Encryption client installers.
- Preparing your end users for a successful installation.

This Guide assumes you have already read the Symantec Encryption Management Server Administrator's Guide and have installed and used a Symantec Encryption Management Server.

Note: Symantec Corporation strongly recommends you take the time to understand your goals for the software products available from Symantec Corporation and your organization’s plans for them, both now and in the future. The decisions you make now in deploying Symantec Drive Encryption affect how you can do things in the future. For example, your choice of key mode now will impact decisions you make later.
Important Terms

**Symantec Drive Encryption:** A software product from Symantec Corporation that secures files stored on protected drives with transparent full disk encryption. It also includes other encryption features. Symantec Drive Encryption is available for Windows, Mac OS X, and Linux systems.

**full disk encryption:** A security industry term for encryption of all data on a drive below the application layer.

**Symantec Encryption Management Server:** A software/hardware product from Symantec Corporation used for configuration and management of Symantec Corporation encryption applications, including Symantec Drive Encryption.

**Whole Disk Recovery Token:** A feature of Symantec Drive Encryption where a recovery token is created that can later be used to recover access to a drive if the normal authentication method is no longer available.

**key mode:** One of the four "modes" in which a PGP keypair can be created. Different key modes are more appropriate for different usage scenarios, so be sure to pick the key mode most appropriate for your needs.

**LDAP directory synchronization:** an optional feature of Symantec Encryption Management Server that lets the server query your organization’s LDAP directory server (a Microsoft Active Directory server, for example), thus taking advantage of existing information about configured users and their authentication credentials.

**enrollment:** A process during installation of Symantec Drive Encryption client software where the Symantec Drive Encryption client synchronizes with the Symantec Encryption Management Server. The enrollment process establishes the relationship between the client and the server, binding the managed client to the specific Symantec Encryption Management Server. During enrollment, and when appropriate afterwards, the Symantec Drive Encryption client receives encryption keys, policies, and management updates from the Symantec Encryption Management Server.

Other Relevant Resources

**Note:** This document focuses on details surrounding deployment of the Symantec Drive Encryption product. However, the first step in deploying Symantec Drive Encryption is to install and configure the Symantec Encryption Management Server product, which you will use to manage your Symantec Drive Encryption clients. Deployment of the Symantec Encryption Management Server itself is described at a very high level in this document. Refer to the *Symantec Encryption Management Server Administrator’s Guide* for detailed deployment information.

Use this *Symantec Drive Encryption Deployment Guide* in conjunction with the following resources:
Symantec Encryption Management Server Administrator’s Guide: This guide explains how to set up the Symantec Encryption Management Server you will be using as a management console. Specifically, the Symantec Encryption Management Server Administrator’s Guide describes configuring your Symantec Encryption Management Server, using the server to establish settings for your Symantec Drive Encryption clients, and creating Symantec Drive Encryption client installers.

Symantec Encryption Management Server Installation Guide: This guide describes how to install the Symantec Encryption Management Server software onto a system.

Symantec Drive Encryption Quick Start Guide (QSG): This guide introduces you to the features of the Symantec Drive Encryption product. Consider distributing the Symantec Drive Encryption QSG to your end users to introduce them to the product.

Symantec Drive Encryption Desktop User’s Guide: This guide describes how to use Symantec Drive Encryption on Windows and Mac OS X systems. If you want more information about the Symantec Drive Encryption product than is provided in the Symantec Drive Encryption QSG, consult the Symantec Drive Encryption Desktop User’s Guide.

Symantec Drive Encryption for Linux User’s Guide: This guide describes how to use Symantec Drive Encryption on Linux systems.

Online help: Both the Symantec Encryption Management Server and Symantec Drive Encryption include built-in online help.

Knowledge Base Articles: For specific information about Symantec Drive Encryption and Symantec Encryption Management Server, access the Symantec Knowledgebase (http://www.symantec.com/business/support/index?page=home) and search for particular topics.

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:

www.symantec.com/business/support/

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
• Information about upgrade assurance and support contracts
• Information about the Symantec Buying Programs
• Advice about Symantec's technical support options
• Nontechnical presales questions
• Issues that are related to CD-ROMs or manuals

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, Africa  semea@symantec.com
North America, Latin America  supportsolutions@symantec.com
Understanding Symantec Drive Encryption

This section tells you about Symantec Drive Encryption and shows a typical Symantec Drive Encryption deployment.

In This Chapter

About Symantec Drive Encryption........................................................................................................ 9
Components of a Typical Symantec Drive Encryption Deployment.......................... 10
How Does Symantec Drive Encryption Work? ................................................................. 10
About Symantec Encryption Management Server............................................................. 11

About Symantec Drive Encryption

Symantec Drive Encryption is a software product from Symantec Corporation that secures files stored on protected drives with transparent full disk encryption. If a protected system is lost or stolen, data stored on the protected drive is completely inaccessible without the proper authentication.

Note: Symantec Drive Encryption runs on Windows, Mac OS X, and Linux systems. Only Intel-based systems running Mac OS X 10.4.10 or later support whole disk encryption of the boot disk. Symantec Drive Encryption on Linux systems has a command-line interface and supports whole disk encryption functionality only.

The Symantec Drive Encryption product also provides the following functionality for your Windows and Mac OS X users:

- Use part of your hard drive space as an encrypted virtual disk volume with its own drive letter.
- Create secure, encrypted Zip archives.
- Put files and folders into a single encrypted, compressed archive that can be opened on Windows systems that do not have Symantec Drive Encryption or Symantec Encryption Desktop installed.
- Completely destroy files and folders so that even file recovery software cannot recover them.
- Securely erase free space on your drives so that deleted data is truly unrecoverable.

Symantec Drive Encryption is both a product sold by Symantec Corporation and a feature in several Symantec Corporation products.

When this Guide refers to "Symantec Drive Encryption," it refers to the Symantec Drive Encryption product. Bear in mind, however, that "whole disk encryption" is only one feature of the Symantec Drive Encryption product on Windows and Mac OS X systems. On Linux systems, whole disk encryption is the only feature.
Components of a Typical Symantec Drive Encryption Deployment

The following are elements of a typical Symantec Drive Encryption deployment:

1. **Symantec Drive Encryption** is a software product that locks down the contents of your system. To deploy Symantec Drive Encryption, you must install the Symantec Drive Encryption software on a client system via a customized installer you create using the Symantec Encryption Management Server.

2. **Symantec Encryption Management Server** is a platform for creation and management of Symantec Corporation encryption applications, including Symantec Drive Encryption. The Symantec Encryption Management Server must be able to communicate with your Symantec Drive Encryption clients so that it can:
   - Provide a pre-configured installer for the system
   - Enroll and bind the client to the server
   - Provide and enforce policies
   - Provide recovery options

3. **Directory/LDAP Server** (for example, Active Directory). An LDAP server:
   - Provides an authentication mechanism during Symantec Drive Encryption client enrollment/installation
   - Enables you to synchronize groups for policy application
   - Leverages existing information about the user (email, DN, user certificates, and so on)

4. Your **DNS server** needs to be configured to support your Symantec Encryption Management Server; be sure to coordinate with your IT group to ensure a successful installation.

How Does Symantec Drive Encryption Work?

The following steps are an overview of the Symantec Drive Encryption encryption process and subsequent user experience.

1. The Symantec Drive Encryption passphrase or token user encrypts the boot drive on their system automatically or manually.

2. The drive is transparently encrypted sector by physical sector.

3. Once encryption begins, and thereafter, the Symantec Drive Encryption user must authenticate using the PGP BootGuard screen.

4. To access the system, the user enters a passphrase or inserts their USB token (Windows and Mac OS X systems only) and then authenticates.
If the Single Sign-On feature is enabled on Windows systems, the system automatically logs in to Microsoft Windows.

System behavior is the same as it was prior to encryption.

---

**About Symantec Encryption Management Server**

*Symantec Encryption Management Server* is a platform for central management and deployment of Symantec Corporation encryption applications, including Symantec Drive Encryption. You use the Symantec Encryption Management Server to configure Symantec Drive Encryption client options, provide custom policies and settings for your Symantec Drive Encryption users, create the client installers, and manage the clients after installation (including Whole Disk Recovery Tokens for each managed client, for example).
Major Steps

This guide is organized into sections that correspond with the order Symantec Corporation recommends you use to deploy Symantec Drive Encryption. Depending on your environment, you may perform some of these tasks in a slightly different order.

This guide covers the steps to take to configure and deploy Symantec Drive Encryption clients using a Symantec Encryption Management Server as the management console:

1. **Preparation.** Learn what you need to do **before** you install the Symantec Encryption Management Server, including:
   - Where to put your Symantec Encryption Management Server in your network
   - What you need to know to add the Symantec Encryption Management Server to your network
   - How to configure your firewall to support the Symantec Encryption Management Server
   - How to choose the enrollment method your Symantec Drive Encryption users will use
   - How to set up LDAP directory synchronization (if applicable)

2. **Installation and configuration.** Describes the process of installing the Symantec Encryption Management Server software and steps you through the configuration wizard. All Symantec Encryption Management Server setups go through this process, but there are some things specific to deployments.

3. **Configuring the Symantec Encryption Management Server.** Describes the features of your Symantec Encryption Management Server that impact your deployment:
   - Directory synchronization
   - Enrollment
   - Administrative user email setup
   - Automated backups
   - Removal of unneeded services
   - Other desirable services
   - Policies

4. **Setting Symantec Drive Encryption client options.** Summarizes the Symantec Drive Encryption settings you control so that you can appropriately configure them to reflect your organization's security requirements.

5. **Creating the Symantec Drive Encryption client installer.** Describes the process of creating the actual client installer executable.

6. **Testing the client installer.** Lists ways you can test your client installer before full deployment.

7. **Deploying the client installer to end users.** Provides options for deploying the client installer executable to your end users.
8  **Assisting your users.** Discusses some of the things you can do to help prepare your end users for the new software they will be receiving.
Preparation

Preparation consists of things you need to do or to understand before you begin installing your Symantec Encryption Management Server as your management console:

- Where to put your Symantec Encryption Management Server in your network
- What you need to know to add the Symantec Encryption Management Server to your network
- How to configure your firewall to support the Symantec Encryption Management Server
- Understanding the LDAP Directory Synchronization feature
- Understanding policy options
- Understanding enrollment methods
- Making sure the systems on which Symantec Drive Encryption will be installed are appropriately prepared

In This Chapter

Placing the Symantec Encryption Management Server in your Network............ 15
Adding the Symantec Encryption Management Server to your Network............ 16
Configuring your Firewall..........................................................................................17
Understanding Enrollment..........................................................................................18
Understanding the Two Enrollment Paths ...............................................................18
Understanding the LDAP Directory Synchronization Feature...............................19
Understanding Policies ............................................................................................19
Preparing End-User Systems....................................................................................20

Placing the Symantec Encryption Management Server in your Network

For ease of deployment, you can place your Symantec Encryption Management Server in your DMZ. If you are deploying the Symantec Encryption Management Server in this fashion, Symantec recommends that you take the following actions:

- Secure your private keys and encrypt your server. Two ways of securing your private keys are using a hardware token Ignition Key or using a Hardware Security Module (HSM).

**Note:** Use of an HSM requires Symantec Technical Support involvement.
Preparing the Symantec Encryption Management Server to your Network

- Remove or disable unneeded services. See Removing Unneeded Services (on page 23).
- Adjust your firewall configuration and remote access ports. See Configuring your Firewall (on page 17).
  - Adjustments protect the confidentiality of your data. This includes blocking all administrative ports listed in Configuring your Firewall.
  - If you will be using the LDAP enrollment feature of Symantec Encryption Management Server, you must have connectivity through your firewall, from your DMZ into your corporate network. This connectivity may require firewall, proxy, and/or network configuration changes. Connectivity allows both internal and external user access to the Symantec Encryption Management Server. This access is essential, for example, if you have laptop users who travel and may not have access to the VPN when they install the Symantec Drive Encryption client.

For details on potential configurations and tasks involved in placing your server, see the Symantec Encryption Management Server Installation Guide.

Adding the Symantec Encryption Management Server to your Network

Once you have determined a network location for your Symantec Encryption Management Server, you must do the following:

**Note:** You may need to consult with your network and/or system engineering teams to support the deployment of your Symantec Encryption Management Server.

- Assign an appropriate IP address to the Symantec Encryption Management Server.
- Configure the appropriate subnet and gateway.
- Configure the appropriate hostname and DNS.

**Note:** The use of DNS forward and reverse pointers is required; using a hosts file is not sufficient.

Make sure the DNS includes appropriate A and PTR records that are in place prior to installation of the Symantec Encryption Management Server.

Also, make sure the DNS is reachable by the Symantec Encryption Management Server, if it is in the DMZ.

Deployment Options

There are other options to consider at this point:

- Do you want to replace the default self-signed server SSL certificate with a real SSL certificate?
Symantec Corporation strongly recommends that you obtain a valid SSL/TLS certificate for each of your Symantec Encryption Management Servers from a public Certificate Authority (CA), such as GeoTrust. This ensures that clients will have confidence in establishing secure communications with your servers. An in-house CA will not be recognized by the Symantec Drive Encryption client.

- Are you going to use DNS round robin or a load balancer with your Symantec Encryption Management Server?

If so, acquire the proper number of IP addresses or VIP addresses required for each machine in the cluster as well as proper DNS forward and reverse pointers. Getting this information in advance will help to ensure a smooth implementation.

---

### Configuring your Firewall

The Symantec Drive Encryption clients you are deploying will be in contact with your Symantec Encryption Management Server on a regular basis. They must be able to communicate with each other; otherwise, many aspects of your deployment will not work. Also, the management console needs certain ports open on your firewall for a variety of purposes.

Firewall changes should be done before you install the Symantec Encryption Management Server.

Specifically:

- Clients must be able to access the management server using HTTPS on port 443; allow traffic in both directions. This also includes traffic from the Internet with a destination of port 443 to the Symantec Encryption Management Server, if you are deploying the server in your DMZ.

- If you deploy the Symantec Encryption Management Server in your DMZ and you are using LDAP enrollment, allow port 636 (LDAPS) or port 3269 (Global Catalog Server SSL) access to your supported LDAP server.

- The management server must be able to make LDAP and LDAPS queries on ports 389 and 636, respectively, to the LDAP server you are using for directory synchronization.

- If you are using email enrollment, no LDAP connectivity is required internally, but external LDAP access may be required to support other Symantec Drive Encryption functionality: key lookups or file/folder encryption, for example.

- The management server needs FTP or SCP access on ports 21 or 22, respectively, for delivery of backups to an appropriate location.

- Regular backups are important to support the ability to recover from unexpected failure of the Symantec Encryption Management Server. Symantec Corporation strongly recommends you set up regular schedule of backups of the data on your Symantec Encryption Management Server.

- You will be configuring the Symantec Encryption Management Server you are using as a management server via its web-based administrative interface using HTTPS on port 9000, so this port needs to be open.

- Enabling SSH access to the management server on port 22 will give you access should web-based access be down for some reason.
Understanding Enrollment

Symantec Drive Encryption clients synchronize with their Symantec Encryption Management Server during installation through the client enrollment process. Once enrolled with their Symantec Encryption Management Server, clients receive encryption keys, policies, and management updates from the Symantec Encryption Management Server. The enrollment process establishes the relationship between the client and the server, binding the managed client to the specific Symantec Encryption Management Server.

There are two methods for enrolling your Symantec Drive Encryption users:

- **LDAP Directory Synchronization**: Requires that the LDAP Directory Synchronization feature be enabled (and correctly configured) and the **Enroll clients using directory authentication** checkbox be selected on the Directory Synchronization screen in the Symantec Encryption Management Server's management interface. To enroll, the client will provide authentication credentials to the LDAP directory specified in the LDAP Directory Synchronization feature.

- **Email**: Requires only that the Symantec Drive Encryption client and the Symantec Encryption Management Server are able to communicate using SMTP email. This method is available for all client installations, provided there is a usable email account on the client system. This method is available even if the Symantec Encryption Management Server is not performing email encryption. To enroll with a server, the client sends an email to the Symantec Encryption Management Server. The Symantec Encryption Management Server processes the email message and then sends an email message back to the Symantec Drive Encryption client. The client uses the return email to finalize the enrollment process and then continues with the installation.

Understanding the Two Enrollment Paths

There are two basic "paths" for deciding how to configure the LDAP Directory Synchronization feature, policies, and enrollment methods:

- If you have an up-to-date LDAP directory server in your organization, you will probably want to enable the LDAP Directory Synchronization feature (and turn enrollment on), select **Auto detect policies**, and use the LDAP Directory Synchronization feature for enrollment. This leverages the information in your LDAP directory and simplifies the job of the administrator.

- If you do not have an up-to-date LDAP directory server in your organization, you will want to keep the LDAP Directory Synchronization feature disabled, select **Preset policy**, and use email enrollment.

- Notification emails from the management server to administrators of the Symantec Encryption Management Server are sent via SMTP on port 25, so that port should be open between the Symantec Encryption Management Server and the mail server that will accept email from administrators.
Understanding the LDAP Directory Synchronization Feature

LDAP Directory Synchronization is a feature of Symantec Encryption Management Server which, if enabled (it is disabled by default), can be used with your Symantec Drive Encryption deployment. Enabling this feature lets your Symantec Encryption Management Server query your organization's LDAP directory server for information about users and import the appropriate users, thus taking advantage of existing information about users and their authentication credentials.

**Note:** Proper LDAP syntax must be used when you work with the LDAP Directory Synchronization feature.

There are three LDAP Directory Synchronization configuration options:

- **LDAP Directory Synchronization enabled, enrollment on.** The specified LDAP directory will be used to determine which users are in what groups for the purposes of applying the appropriate policy and for enrollment.

- **LDAP Directory Synchronization enabled, enrollment off.** The specified LDAP directory will be used to determine which users are in what groups for the purposes of applying the appropriate policy, but **not** for enrollment purposes. (Email enrollment will be used.)

- **Disabled.** LDAP Directory Synchronization is disabled; the Symantec Encryption Management Server will not check any LDAP directories in your organization either for users to be imported or for enrollment. (Email enrollment will be used.)

Understanding Policies

There are three methods available to determine how your Symantec Drive Encryption users will receive internal user policies from the Symantec Encryption Management Server; which one you choose depends on your particular circumstances.

The three policy methods are:

- **No policy.** Your Symantec Drive Encryption users can do anything their license allows; they will not receive any policies from the Symantec Encryption Management Server console.

- **Auto-detect policy.** Your Symantec Drive Encryption users are constrained by the policy that applies to the LDAP directory group they are in. (This option requires that you enable the LDAP Directory Synchronization feature.) Using this policy option means that the most appropriate policy will be selected automatically and applied for the LDAP directory group your users are in. Users could have a different policy applied in the future if a new policy is created that is more appropriate for their LDAP directory group.
• **Preset policy.** Your Symantec Drive Encryption users are constrained by the settings of the selected preset policy, either default policy or a custom policy you create. The consumer policy applies to the installer you create. You can change the settings of the selected preset policy in the future and the new settings will apply to the users constrained by the policy, with the exception of actions taken at installation.

---

**Preparing End-User Systems**

**Note:** Symantec Corporation strongly recommends you check the Symantec Encryption Desktop, Symantec Drive Encryption, and Symantec Encryption Management Server Release Notes to make sure the systems in your deployment environment are ready for installation of both the server and Symantec Drive Encryption client.

As part of your installation preparation:

• Make sure clients meet the listed minimum system requirements.

• Determine whether the email clients used in your environment are supported clients.

• Verify that your anti-virus and firewall software is compatible.

• Review the list of known software conflicts and ensure you will not encounter these in your deployment.

• Ensure that target client systems include scandisk (Windows chkdsk.exe, for example, or SpinRite or Norton Disk Doctor, if available) and defragmentation (Windows defrag.exe, for example, or PerfectDisk, if available) software, for preparing their drives for installation of Symantec Drive Encryption.
Installation and Configuration

This section describes the installation process at a high level. For a more detailed description of each activity, see the Symantec Encryption Management Server Administrator's Guide.

In This Chapter

Before You Install ................................................................. 21
Installing the Server Software ............................................. 21

Before You Install

Before you install the software, ensure you have the following available to you:

- The appropriate hardware on which to install the Symantec Encryption Management Server software. The current Symantec Encryption Management Server Certified Hardware List is located in the most recent version of the Symantec Encryption Management Server Release Notes.
- The most recent version of the Symantec Encryption Management Server software.
- The most recent version of the Symantec Encryption Management Server Administrator's Guide.

Note: To view the most recent version of the Symantec Encryption Management Server Release Notes and the Symantec Encryption Management Server Administrator's Guide, please go to the Products section on the Symantec Corporation Web site (http://www.symantec.com/business/support/).

Installing the Server Software

1. Perform the default installation of the Symantec Encryption Management Server software, as described in the Symantec Encryption Management Server Installation Guide.

2. Configure the server using the Setup Assistant. Connect to the Symantec Encryption Management Server when the standard installation is complete, as described in the Symantec Encryption Management Server Installation Guide.

3. On the Welcome screen, read the text, then click the Forward arrow to continue.
4 On the End User License Agreement screen, read the text of the License Agreement, then click the I Agree button.

5 On the Setup Type screen, select New Installation, then click the Forward arrow to continue.

6 On the Date & Time screen, enter the appropriate information, then click the Forward arrow to continue.

7 On the Network Setup screen, verify that the information you entered in the standard installation is correct, and then click the Forward arrow to continue.

8 On the Confirmation screen, verify that the information is correct, and then click Done.

The server reboots.

9 When the Licensing screen appears, enter the appropriate licensing information for the Symantec Encryption Management Server you are using as a management console.

**Note:** The Enable Mail Proxies check box must be selected to configure and use mail proxies.

10 Click Save.

11 On the Administrator Name & Passphrase screen, enter the appropriate information, and then continue.

12 If you selected the Enable Mail Proxies check box on the Licensing screen, the Mail Processing screen appears. Select Gateway Placement, and then continue.

13 On the Mail Server Selection screen, enter the appropriate information, and then continue.

14 On the Ignition Keys screen, make the desired selection, and then continue.

15 On the Ignition Keys screen that appears, enter the appropriate information, and then continue.

16 On the Backup Organization Key screen, enter a passphrase to protect your Organization Key, then click Backup Key. An Organization Key will be generated. This key allows you to restore your Symantec Encryption Management Server from a backup, should that be necessary. (The other use of an Organization Key, to sign the keys created by the Symantec Encryption Management Server, does not apply if you are using the Symantec Encryption Management Server only as a management server.)

17 When the Confirmation screen appears, check to make sure the settings are correct, and then click Done.
Configuring the Symantec Encryption Management Server

There are multiple aspects of the Symantec Encryption Management Server that you should configure to get it ready for use as a management console:

- Removing unneeded services
- Setting up administrators
- Establishing settings for backups
- Securing the server
- Configuring policies
- Configuring the LDAP Directory Synchronization feature (if applicable)
- Configuring enrollment

In This Chapter

Removing Unneeded Services ................................................................. 23
Setting Up Administrators ........................................................................ 24
Establishing Backups ............................................................................... 24
Securing your Symantec Encryption Management Server ....................... 25
Configuring Policies ............................................................................... 25
Configuring the LDAP Directory Synchronization Feature ...................... 26
Configuring Enrollment ......................................................................... 27

Removing Unneeded Services

Some services provided by the Symantec Encryption Management Server are unnecessary if the server is being used only as a management console for Symantec Drive Encryption clients. Symantec Corporation recommends modifying the default settings of these services, as described below, for optimal operation of your management console.

Do the following:

- Navigate to Mail > Proxies and delete the SMTP proxy; it is not needed.
- Navigate to Mail > Mail Routes. Delete all existing entries and add a new entry with an asterisk (*) as the domain name and the IP address of the mail server that will accept mail for delivery from the Symantec Encryption Management Server. This will force the Symantec Encryption Management Server not to use DNS for mail queries; instead, it will send all mail to the specified mail route.
- Navigate to Services > Web Email Protection. Click Disable to deactivate the service.
- Navigate to Services > Keyserver. Click Disable to deactivate the service.

Your Symantec Encryption Management Server offers a number of other services that you may or may not want to activate if you are using the server only as a management server. For more information about these services, see the Symantec Encryption Management Server Administrator’s Guide.

### Setting Up Administrators

Symantec Encryption Management Servers allow multiple administrators and support different roles for administrators. You can set up an administrator whose access would be limited to handling just Whole Disk Recovery Tokens, for example.

During installation, you create one administrator; this administrator is a superuser, which means they have access to all Symantec Encryption Management Server functionality.

To create additional administrators:

1. From the System > Administrators card, click Add Administrator.
2. In the Login Name field, enter a login name for the new administrator.
3. In the Passphrase field, enter a passphrase for this administrator.
4. In the Confirm field, enter the same passphrase again.
5. In the Email field, enter the email address of the new administrator.
6. Select the Daily Status Email checkbox if you want the new administrator to receive a daily status email for your system.
7. From the Role list, select the role for the new administrator. The privileges for the selected role appear.
8. Click Save. The new administrator is added.

For more information about administrators, see the Symantec Encryption Management Server Administrator’s Guide.

### Establishing Backups

Symantec Encryption Management Server provides two ways to back up your data: scheduled backups and on-demand backups. Backup files can be stored on the Symantec Encryption Management Server, or they can be automatically sent using FTP or SCP, to a location you specify.

To establish automatic backups

1. Navigate to the System > Backups screen of the administrative interface, and click Backup Schedule. The Backup Schedule dialog appears.
2. Select Enable Scheduled Backups if it is not already selected.
3. Select the boxes representing the names of the days of the week on which you want backups performed.
4 Specify a time for the backups to begin in the **Start backups at** field.
5 Click **Save**.

**To perform an on-demand backup**

1 Navigate to the **System > System Backups** screen of the administrative interface.
2 Click **Backup Now**.
3 Enter a **Backup Name** and click **Backup**.
   - A backup of your data is performed immediately. When the backup is complete, it displays in the **Backups** list.

For more information about backups, see the **Symantec Encryption Management Server Administrator’s Guide**.

---

**Securing your Symantec Encryption Management Server**

You can use hardware or software Ignition Keys to protect the data on your Symantec Encryption Management Server:

- **Hardware Token Ignition Keys.** When you insert a PKCS#11 token in the Symantec Encryption Management Server, the Symantec Encryption Management Server will detect it and allow you to use it as an Ignition Key. The token must contain a single key, which must be protected by a PIN. You can cache the token’s PIN so that you do not need to enter the PIN at restart, just have the token present.

- **Soft-Ignition Passphrase Ignition Keys.** A passphrase you specify protects the Symantec Encryption Management Server.

**Note:** Symantec recommends that you use the hardware version.

For more information about Ignition Keys, see the **Symantec Encryption Management Server Administrator’s Guide**.

---

**Configuring Policies**

As administrator, you control a variety of settings on the Symantec Drive Encryption software your end users will be using, including key settings, Symantec Drive Encryption client settings, directory services, client updates, and proxy server settings.

These policies are called consumer policies; the settings here control how your Symantec Drive Encryption users will use the product. These policies have nothing to do with the mail processing policies that can also be configured on a Symantec Encryption Management Server.

To begin configuring policies for your Symantec Drive Encryption end users, navigate to **Consumers > Consumer Policy**. The **Consumer Policy** page appears.

By default, one internal user policy is always created: **Default**.

You have several options at this point:
Configure the default **Default** policy so that it conforms to your organization's security policies and use that policy for your Symantec Drive Encryption users.

- Create a new consumer policy, configure that policy so that it conforms to your organization's security policies, and then use the new policy for your Symantec Drive Encryption users.
- Create multiple new consumer policies, configure them appropriately, and then use them for your Symantec Drive Encryption users. For example, if your organization's security policies call for stronger security for executives or certain departments, you could create multiple internal user policies to support this.

To configure consumer policies, refer to *Establishing Symantec Drive Encryption Client Settings* (on page 29).

For more information about these settings, refer to the *Symantec Encryption Management Server Administrator's Guide*.

---

**Configuring the LDAP Directory Synchronization Feature**

If you have an up-to-date LDAP directory server in your organization, you will probably want to enable the LDAP Directory Synchronization feature on your Symantec Encryption Management Server so that you can use your LDAP server for auto-detecting polices and enrollment. This both leverages the information in your LDAP directory and simplifies the job of the administrator.

**To enable the LDAP Directory Synchronization feature**

1. Navigate to the **Consumers > Directory Synchronization** screen in the administrative interface. The **Directory Synchronization** page appears.

2. Select **Enable** if LDAP Directory Synchronization is disabled.

3. Click **Add LDAP Directory**.

4. In the **Name** field, enter a name for the LDAP directory you are adding.

5. From the **Type** drop-down menu, select the type of directory: choose **Active Directory** or **OpenLDAP (RFC 1274)**. Active Directory is the default setting. Microsoft Active Directory uses the sAMAccountName attribute for user information. OpenLDAP-based directories use the attribute uid for user information. Symantec Encryption Management Server queries user information using only the necessary attributes, providing faster results when querying user information.

6. In the **Bind DN** field, type the Distinguished Name of a valid user that exists in the LDAP directory. Symantec Encryption Management Server will use this as the user name to bind (log in) to the LDAP directory. This DN must match the name of an existing user in the directory. Binding determines the permission granted for the duration of a connection.

7. In the **Passphrase** field, type the passphrase to use for authentication to the DN. If you want to bind to the LDAP directory anonymously, leave these fields blank. If no DN is provided, Symantec Encryption Management Server will attempt to bind anonymously.

8. Go to the **LDAP Servers** tab and add at least one LDAP server.
9 Go to the **Base Distinguished Names** tab to specify any Base DNs you want to use as the basis for searches within this directory.

10 Go to the **Consumer Matching Rules** tab if you want to set rules for which email addresses should be searched for in this LDAP directory.

11 Click **Save**.

---

### Configuring Enrollment

As described previously, there are two methods available for enrollment:

- **Email (the default).** Requires only that the Symantec Drive Encryption client and the Symantec Encryption Management Server be able to communicate via SMTP email. This method is available for all client installations, as long as there is a usable email account on the client system, even if the Symantec Encryption Management Server is not performing email encryption or is out of the mailflow.

- **LDAP Directory Synchronization.** Requires that the LDAP Directory Synchronization feature be enabled (and correctly configured) and that the “Enroll clients using directory authentication” option be selected on the Directory Synchronization page. To enroll, the client will provide authentication credentials to the LDAP directory specified in the LDAP Directory Synchronization feature.

The following information is common to both methods of enrollment:

- Port 443 must be open between your Symantec Drive Encryption clients and the Symantec Encryption Management Server. This is the port the Symantec Drive Encryption clients use to get policy and receive encryption keys. Enrollment will fail if port 443 is blocked.

- On the **Consumers > Managed Domains** screen, make sure that your managed domain matches the domain you use for email. **You must do this even if you are not using the messaging functionality of the Symantec Encryption Management Server.** For example, if you have an email address of jsmith@eng.example.com and the managed domain configured on your Symantec Encryption Management Server is example.com, enrollment will not work because the domain does not exactly match what is configured on the Symantec Encryption Management Server. It is possible to configure multiple email domains on the Symantec Encryption Management Server; configuring eng.example.com as an additional domain would solve the problem.

- Make sure you have DNS properly configured, including pointer records, or enrollment may fail.

---

### Email Enrollment

To configure email enrollment:

- Navigate to the **Mail > Mail Routes** screen on your Symantec Encryption Management Server and add a route from the protected domain to the hostname of your mail server. For example, you could use the domain name eng.example.com and the mail server address hostname/IP mail.eng.example.com.
If you have already configured a mail route using an asterisk (*) as the domain name and the IP address of the mail server that will accept mail for delivery from the Symantec Encryption Management Server, you do not need to configure another mail route.

- Make sure port 25 is open between your Symantec Encryption Management Server and your mail server and make sure your mail server accepts SMTP (Domino servers might not by default, for example).

When your Symantec Drive Encryption users install Symantec Drive Encryption on their systems, an Enrollment Assistant will appear, asking them to open their email client, check for new messages, and open the enrollment email message the management server sends them. It is critical that your users open the message, as it puts a cookie onto their system. This cookie is required for the successful completion of the enrollment process.

LDAP Directory Synchronization Enrollment

You may want to use tools such as ADSIedit (from the Windows Support tools section of your Server OS CD) or SoftTerra’s ldapbrowser from ldapbrowser.com to facilitate LDAP Directory Synchronization enrollment. This ensures that proper LDAP syntax is used.

Your directory schema must contain certain attributes for you to use LDAP Directory Synchronization enrollment. Every user is required to have an email address in the attribute mail.

Other settings to check include:

- cn, mail
- smtpProxyAddress (or proxyAddress SMTP)
- uid
- sAMAccountName
- Usercertificate
- binary

All these attributes (except Usercertificate and binary) need to be present in the directory. The attribute of your LDAP filter needs to be present as well.

When your Symantec Drive Encryption users install Symantec Drive Encryption on their systems, they will be prompted for their username and password on the LDAP directory. Ensure that they do this, as it is required for the successful completion of the enrollment process.
Establishing Symantec Drive Encryption Client Settings

The Symantec Drive Encryption client is installed on each system in your deployment. Consider the following topics when planning to configure Symantec Drive Encryption clients:

- Specifying the appropriate key settings
- Establishing Symantec Encryption Desktop settings for your clients
- Configuring other internal user policy settings

**Note:** There are a few features of Symantec Drive Encryption that are supported on Windows systems but not on Mac OS X or Linux systems. If you configure these features for your Windows clients and also create Mac OS X and/or Linux clients, the settings for these features will be ignored on the Mac OS X and Linux systems; all other settings will work normally.

In This Chapter

General Settings ............................................................................................................ 29
Key Settings ................................................................................................................... 30
Symantec Encryption Desktop Settings ............................................................................ 34
Licensing Settings ......................................................................................................... 44

---

**General Settings**

These settings are found on the three tabs at the bottom of the Policy Options page *(Consumers > Consumer Policy > [policy] > General > Edit)*.

The Directory Services tab of the Policy Options page is different depending on whether you are editing the Everyone group Consumer Policy or a policy you created.

- If you are editing a user-created policy, you can assign policies to internal users based on their directory attributes, if the LDAP Directory Synchronization feature is enabled. Refer to the *Symantec Encryption Management Server Administrator's Guide* for more information.

- **Notify users of software updates and automatically download.** Select if you want your Symantec Drive Encryption client to have updated software clients automatically downloaded.

- **Use an HTTPS Proxy Server for Symantec encryption client communications.** Select if your Symantec Drive Encryption clients connect to the Symantec Encryption Management Server through a proxy server.
  - **Hostname.** Enter the hostname of the HTTPS proxy server.
  - **Port.** Enter the port used to access the HTTPS proxy server.
Establishing Symantec Drive Encryption Client Settings

Key Settings

These settings apply to the PGP keys that your Symantec Drive Encryption users can create. The settings are found on the tabs of the Symantec Encryption Management Server console (Consumers > Consumer Policy > [policy] > Keys > Edit).

Key Generation Settings

The settings on the Generation tab:

- **Type**: Select the default key type for your Symantec Drive Encryption users, either RSA or DH/DSS. The default is RSA.
- **Generate separate signing subkey**: Check if you want your Symantec Drive Encryption users to be able to generate separate signing subkeys.
- **Key Size**: Select the default key size for your Symantec Drive Encryption users. Available options are 1024, 1536, 2048, 3072, and 4096.
- **Supported Ciphers**: Deselect any cipher you do not want your users to be able to use.
- **Preferred Cipher**: Select the cipher you want your end users to use if no algorithm is specified; you can select any supported cipher. The default is AES.
- **Supported Hashes**: Deselect any hash type you do not want your end users to be able to use.
- **Preferred Hash**: Select the hash you want your end users to use if no hash is specified; you can select any supported hash. The default is SHA-2-256.
- **Supported Compression**: Deselect any compression type you do not want your end users to be able to use. None means data will not be compressed before it is encrypted.
- **Preferred Compression**: Select the compression type you want your end users to use if no compression type is specified; you can select any supported compression type. The default is ZLIB.
- **Auto-Renew Keys Every**: Select an auto-renewal time frame for the keys of your Symantec Drive Encryption users. Internal keys will automatically be renewed in the time frame you specify unless they have exceeded the inactivity threshold in Stop Renewing After. Select Never renew if you want your internal keys never to renew; this means the keys will never expire, regardless of inactivity.

- **Additional Decryption Key**: Click the Import button and select a key to be used as an Additional Decryption Key for this consumer policy.
- **Edit XML Preferences**: Clicking the Edit Preferences button lets you edit XML policy preferences. Do not use the XML Preferences Editor without help from Symantec Support. Misconfiguring the preferences can cause your Symantec Drive Encryption installations to stop working properly.
Establishing Symantec Drive Encryption Client Settings

Key Settings

- **Stop Renewing After**: Specify a period of inactivity after which a key will not be automatically renewed. Select **Never stop renewing** if you want keys of your Symantec Drive Encryption users to be continually renewed. The question you should ask yourself here is how long a period of inactivity for a given user should be before you reasonably conclude that the user account is no longer in use.

It is generally a good idea to set the auto-renewal time to be fairly short. This helps ensure that the Symantec Encryption Management Server manages itself without you needing to delete a user manually in the event someone leaves your organization.

**Key Mode Settings**

The options on the Management tab let you select which key modes your Symantec Drive Encryption users will be able to select when they create keys. You must allow at least one key mode.

**Note**: The decisions you make now in deploying Symantec Drive Encryption, including selecting a key mode, affect how you can deploy and use other Symantec Corporation products in the future.

Available options are:

- **Server Key Mode (SKM)**. Select this option if you want the Symantec Encryption Management Server to generate and manage the keys of your Symantec Drive Encryption users.
- **Client Key Mode (CKM)**. Select this option if you want your Symantec Drive Encryption users to be able to generate and manage their own PGP keys.
- **Guarded Key Mode (GKM)**. Select this option if you want your Symantec Drive Encryption users to be able to generate and manage their own keys, and you also want encrypted copies of users’ private keys stored on the Symantec Encryption Management Server as a backup for the end user.
- **Server Client Key Mode (SCKM)**. Select this option if you want private encryption keys shared between your Symantec Drive Encryption users and the Symantec Encryption Management Server, and private signing keys stored only on the clients. SCKM supports Symantec Drive Encryption, Symantec File Share Encryption, and PGP Messaging users.

For more information, see the *Symantec Encryption Management Server Administrator's Guide*.

**Certificates Settings**

The settings on the Certificates tab:

- **Use the username as the Common Name (CN)**: Select to have the consumer’s username be the common name to which the certificate is issued.
- **Country (C)**: Select to specify the country.
- **State/Province (ST)**: Select to specify the name of the state or province, as appropriate. Do not abbreviate the state or province name. For example, type "California" not "CA".
- **Locality (L)**: Select to specify the name of the city or locality, as appropriate.
- **Organization (O):** Select to specify the name of your organization or company.
- **Organizational Unit (OU):** Select to specify the name of your organization’s unit, as appropriate.
- **Create end entity certificate (omit BasicConstraints):** Select this option if you do not want to create CA certificates. Deselect this option to create CA certificates.
- **CRL Distribution point:** Select this option to put the CRL distribution point into the certificate. The CRL distribution point is specified from Services > Certificate Revocation.
- **Derive key usage extension values from key:** This setting allows generated certificates to have the same usage flags as are on the matching PGP key.
- **Set non-repudiation key usage:** Non-repudiation is a usage flag specific to X.509 certificates. If you select this option, users with this usage will be able to sign S/MIME messages with non-repudiation. Non-repudiation, which provides assurance of the source and integrity of the message, is required in some environments.

Allowed Key Usages control what usage flags (certificate attributes) a generated certificate is permitted to request, not what usage flags the certificate will actually have.

- **Digital Signature (digitalSignature):** Allows the certificate to have a signing usage flag.
- **Non-repudiation (nonRepudiation):** This setting allows the certificate to contain a non-repudiation usage flag, but does not actually apply the usage flag. Both this setting and Set non-repudiation key usage must be selected for the certificate to be used for non-repudiation.
- **Key Encipherment (keyEncipherment):** Allows the certificate to be used to encrypt other keys or certificates.
- **Data Encipherment (dataEncipherment):** Allows the certificate to be used for encryption.
- **Key Agreement (keyAgreement):** Allows the use of the certificate for key exchange protocols; for example, Diffie-Hellman key exchange.
- **Encipher only (encipherOnly):** Allows the certificate to be used for encryption only.
- **Decipher only (decipherOnly):** Allows the certificate to be used for decryption only.
- **TLS WWW Server Authentication:** Allows the certificate to be used for TLS/SSL server authentication.
- **TLS WWW Client Authentication:** Allows the certificate to be used for TLS/SSL client authentication.
- **Email Protection:** Allows the certificate to protect email messages using S/MIME.
- **Import X.509 certificates as:** Select PGP Bundle Keys, PGP Wrapper Keys, or User selectable.
  - PGP Bundle Keys bundles user X.509 signing and encryption certificates into a single identity. This is the recommended option.
  - PGP Wrapper Keys allows user X.509 signing and encryption certificates to be imported as separate identities. This option is not recommended because it only functions in an exclusively S/MIME environment.
Establishing Symantec Drive Encryption Client Settings

Key Settings

- User selectable allows your Symantec Drive Encryption users to choose how to import their smartcard X.509 certificates.

- **Storage of keys on supported smart cards.** Select **Attempt** or **Require**.
  - **Attempt** means that Symantec Drive Encryption will attempt to store new keys created by your Symantec Drive Encryption users on supported smartcards that are detected, but will not require a supported smartcard in order to create a new key.
  - **Require** means that new keys your Symantec Drive Encryption users create must be stored on a supported smartcard. They will not be able to create a key unless it can be stored on a smartcard.

- **Use of CAPI-based credentials.** Select **Force**, **Prefer**, or **Ignore**.

Options Settings

The settings on the Options tab:

- **Allow users to receive encrypted email.** Enable if you want your Symantec Drive Encryption users to receive encrypted email. Disable to prevent them from receiving encrypted email.

- **Enforce minimum passphrase length of X characters.** Enable if you want to require a minimum number of characters in passphrases for new keys created by your Symantec Drive Encryption users. The default is eight characters.

- **Enforce minimum passphrase quality of X%.** Enable if you want to require a minimum passphrase quality level for new keys created by your Symantec Drive Encryption users.

- Saving passphrases. Select one of the three options that will apply to your end users entering their passphrases:
  - **Save passphrases for the current session only.** Automatically saves passphrases in memory until your end user logs off their computer. If you enable this option, your end users will be prompted for their passphrase once per private key. They will not be prompted to enter it again for the same key until they log off of their computer.
  
  **Caution:** If you select this option, it is very important to tell your end users to log off their computers before leaving them unattended. Passphrases can remain cached for weeks if they never log off, allowing anyone to read their encrypted messages or encrypt messages with their key while they are away from their computer.

  - **Save passphrases for X (hh:mm:ss).** Automatically saves passphrases in memory for the specified duration of time. If you enable this option, your end users will be prompted for their passphrases once for the initial signing or decrypting task; they will not be prompted to enter it again until the specified time has elapsed. The default setting is 0:3:0 (3 minutes).

  - **Do not save passphrases.** Prevents your end users’ passphrases from being stored in memory. If you enable this option, your end users must enter their passphrase each time it is needed.
Establishing Symantec Drive Encryption Client Settings
Symantec Encryption Desktop Settings

Symantec Encryption Desktop Settings

There are multiple ways for you to control what your users can do with Symantec Drive Encryption clients when it is installed on their systems:

- **License settings:** The traditional method of controlling what your users can do with Symantec Drive Encryption clients is for your organization to purchase licenses that support the features you want. So if you want your users to encrypt their drives, you purchase licenses that include support for Symantec Drive Encryption.

- **Feature settings:** Once your organization purchases the appropriate licenses, you establish settings for each feature that support your organization’s security policies. So if Symantec Drive Encryption is supported by license, for example, you can control whether or not removable USB disks inserted on your users’ systems must be encrypted.

- **Feature control:** Another way to control what your users can do with Symantec Drive Encryption clients is by controlling not just the settings for a feature but the feature itself. So if your organization has licenses for all employees that support PGP Shredder, for example, but you have a subset of employees that do not need this feature, you can create a client installer just for this subset of users that does not contain the PGP Shredder feature. Feature control is available for all major features of Symantec Drive Encryption clients. Features that are disabled do not appear in the Symantec Drive Encryption user interface.

- **Component control:** You can also control what your users can do with Symantec Drive Encryption clients by editing the MSI client installer file to disable Symantec Encryption Desktop components (for Windows clients only). If your organization does not use Lotus Notes or Groupwise for messaging, for example, you could disable these components to limit any potential compatibility issues. This is accomplished by using Microsoft’s msiexec application to disable components after the client installer file is created. To re-enable a component that has been disabled requires a reinstallation of Symantec Encryption Desktop with the component enabled. Components that are disabled do not appear in the Symantec Encryption Desktop user interface. See Controlling Symantec Drive Encryption Components (on page 49) for more information.

To establish Symantec Encryption Desktop settings for your Symantec Drive Encryption clients, go to Consumers > Consumer Policy > [policy] > Symantec Encryption Desktop > Desktop. The settings are spread over five tabs.

General Tab

The fields on the General tab control permissions and keys; they also include some general settings. For detailed descriptions of these settings, see the Symantec Encryption Management Server Administrator’s Guide.

The fields on the General tab are:

- **Allow users to change options.** When selected, lets your Symantec Drive Encryption users change the settings that you, their administrator, have established. Deselect this option to prevent them from changing these settings.
- **Allow user-initiated key generation.** When selected, lets your Symantec Drive Encryption users create new keys and subkeys—in addition to the key created during installation. Deselect to prevent them from creating new keys after installation and from making certain changes to their keypairs, such as adding and removing ADKS, appointing and removing third-party key revokers, or creating and using subkeys.

- **Allow user-initiated key signing.** When selected, lets your Symantec Drive Encryption users sign keys. Deselect to prevent them from signing keys. You may need to do this to enforce centralized control over the validity of keys in your organization.

- **Allow conventional encryption and self-decrypting archives.** When selected, lets your Symantec Drive Encryption users conventionally encrypt files using a passphrase instead of a key, or create self-decrypting archives (SDAs). Note that conventionally encrypted and self-decrypting files cannot be decrypted by your organization's ADK, which may conflict with your data recovery policy. Deselect to prevent users from conventionally encrypting files or creating SDAs.

- **Always encrypt to user’s key.** When selected, every message your Symantec Drive Encryption users send will be encrypted to their key. This is in addition to any other user- or system-specified key; for example, the ADK. Deselect if you do not want messages to be automatically encrypted to the user’s key. Users can still manually encrypt their messages to their key.

- **Automatically synchronize keys with servers.** When selected, Symantec Drive Encryption will automatically keep your users' keys synchronized with configured servers (when enabled, user key data synchronizes every 24 hours with the data on the Symantec Encryption Management Server). Deselect this option to prevent automatic synchronization of keys.

- **Automatically set up Key Reconstruction.** When selected, key reconstruction is set up automatically for your Symantec Drive Encryption users when new keys are created. The key reconstruction data is stored on the Symantec Encryption Management Server. Keys created on smartcards and tokens are not compatible with key reconstruction. For information on key reconstruction, see the Symantec Encryption Desktop User’s Guide.

- **Override default keyring locations.** When selected, lets you enter locations for keyrings that override the default locations for Windows and/or Mac OS X systems. This means that your users' keyrings will be created in and backed up to the location(s) you specify instead of the default keyring locations. The default keyring location for Windows is C:\Documents and Settings\[user]\My Documents\PGP\, The default keyring location for Mac OS X is [user]/Documents/PGP/.

- **Enable Silent Enrollment.** When selected, only essential Setup Assistant screens will appear during enrollment; non-essential screens will be suppressed and default settings will be used. This option reduces the number of screens your users must navigate during enrollment.

This option requires both the use of the LDAP Directory Synchronization feature and that the **Allow/Deny/Require encryption of disks to existing Windows Single Sign-On** password option (on the Drive Encryption Tab (on page 39)) be set to **Require.**

- **Activate FIPS 140-2 operational and integrity checks.** When selected, FIPS operational tests will be active on your Symantec Drive Encryption users’ systems the next time Symantec Drive Encryption is started. This may slow performance on those systems.
- **Show Symantec Encryption Desktop in system tray/menu.** When selected, the Symantec Encryption Desktop padlock icon appears in the system tray of your Symantec Encryption Desktop users when Symantec Encryption Desktop is active on their systems. The icon provides access to some Symantec Encryption Desktop features without requiring users to launch the whole application. Deselect to hide the icon.

- **Hide the option to disable PGP Services.** When selected, the Stop PGP Services option will not appear on the PGP Tray menu for your Symantec Drive Encryption users. This prevents your users from using this menu option to disable Symantec Drive Encryption services on their system.

- **Send client logs to Symantec Encryption Server every X minutes.** When selected, specifies how often Symantec Drive Encryption client logs are sent to the associated Symantec Encryption Management Server console. The default is 5 minutes.

- **Download policy updates from Symantec Encryption Server every X hours.** When selected, specifies how often the Symantec Drive Encryption client will download policy updates from the associated Symantec Encryption Management Server console. The default is 24 hours.

### Messaging & Keys Tab

The fields on the Messaging & Keys tab control email messaging, instant messaging, and key management. For detailed descriptions of these settings, see the *Symantec Encryption Management Server Administrator's Guide*.

The fields on the Messaging & Keys tab are:

- **Email Messaging.** Deselect to disable the Email Messaging feature; it will not appear in the user interface.

- **Search for keys on local PGP keyrings when encrypting or verifying email.** When selected, lets your Symantec Drive Encryption users import keys into their keyring so that they can encrypt or verify messages without needing to refer to the Symantec Encryption Management Server for key information. This allows your Symantec Drive Encryption users to operate as if they were not bound to the Symantec Encryption Management Server, even if they are. Deselect to prevent them from searching for keys on their own keyring when encrypting or verifying email.

- **Enable encrypt and sign buttons in Outlook MAPI for Windows.** When selected, buttons for encrypting and signing appear in Microsoft Outlook for your users.

- **Enable Out Of Mail Stream support (OOMS).** When selected, lets your Symantec Drive Encryption users send emails per policy in support of Web Email Protection or Smart Trailers when the Symantec Encryption Management Server is out of the mailstream. When deselected, your Symantec Drive Encryption users will not be able to send these messages if the Symantec Encryption Management Server is out of the mailstream.

- **Allow outbound PGP/MIME from Windows MAPI accounts.** When selected, MAPI uses PGP/MIME to encrypt and verify and sign messages. If this option is not selected, MAPI uses PGP Partitioned. MAPI can send messages PGP/MIME signed whether this setting is enabled or disabled.
- **Add a comment to secured email.** When selected, appends the text in the box to clear-signed PGP blocks, including exported key files, and encrypted files and text. Deselect and leave the box empty if you do not want a comment to be appended to these messages.

- **Sign email stored in IMAP/MAPI sent message folders.** When selected, lets your users choose to either Sign, Encrypt, or Encrypt and Sign messages stored in IMAP/MAPI sent message folders on their systems.

  **Match IMAP folder name patterns.** Symantec Encryption Management Server provides a default list of IMAP sent folder names for supported mail clients. You can add to this list to specify additional IMAP folder name patterns to be secured. You can use a wildcard *.

- **Allow users to follow local client policy.** When selected, lets your Symantec Drive Encryption users take actions that follow local client policy, overriding the mail policy of the Symantec Encryption Management Server. This setting allows users to create messaging policies that could make their messaging less secure. Deselect to prevent users from overriding mail policy.

- **Mail policy.** Lets you control what happens to email when the Symantec Encryption Management Server cannot be reached by Symantec Drive Encryption.
  - Standalone
  - Offline: Standalone
  - Offline: Block
  - Offline: Send Clear

- **If client fails to download policy for X days.** Lets you establish how your Symantec Drive Encryption clients will handle situations where policy cannot be downloaded from the Symantec Encryption Management Server console for the specified period.
  - **Block outbound message.** Outbound messages are blocked when policy cannot be downloaded for the specified period.
  - **Apply last downloaded policy.** The last policy downloaded is used when policy cannot be downloaded for the specified period.

- **Use current PGP issued X.509 certificates instead of existing X.509 certificates.** Select if you are using a Lotus Notes mail server but you want your Symantec Drive Encryption users to use a PGP x.509 certificate as the user’s active certificate in Lotus Notes, but only if the user is already using a non-PGP X.509 certificate. The Lotus Notes certificate is suppressed.

- **Add PGP issued X.509 certificate to Lotus Notes if no X.509 certificate exists.** Select if you want the PGP certificates to be inserted into the Lotus Notes certificate directory, whether the user has another certificate or not. Only available if **Use PGP certificates instead of Lotus Notes certificate** is selected.

- **Prefer Notes native encoding over PGP encoding.** Select if you are using Lotus Notes mail servers with Windows Notes clients and prefer to use native Notes encoding.

- **Instant Messaging.** Deselect to disable the Instant Messaging feature; it will not appear in the user interface.
Establishing Symantec Drive Encryption Client Settings
Symantec Encryption Desktop Settings

- **Encrypt/Decrypt AOL Instant Messenger conversations.** When selected, the instant messages (IMs) between your Symantec Drive Encryption users and other Symantec Drive Encryption or Symantec Encryption Desktop users are protected. Note that IMs will be protected only if both users are running Symantec Drive Encryption or Symantec Encryption Desktop software with this setting enabled. Deselect if you do not want these IM sessions to be protected.

- **Key Management.** Deselect to disable the Key Management feature; it will not appear in the user interface, preventing your users from managing their keys.

### Zip & Shredder Tab

The fields on the Zip & Shredder tab control settings for PGP Zip and PGP Shredder. For detailed descriptions of these settings, see the *Symantec Encryption Management Server Administrator's Guide.*

The fields on the Zip & Shredder tab are:

- **PGP Zip.** Deselect to disable the PGP Zip feature; it will not appear in the user interface and it will be not be available to your users.

- **PGP Shredder.** Deselect to disable the PGP Shredder feature; it will not appear in the user interface and it will not be available to your users.

- **Number of shredder passes.** Enter the number of shredder passes your Symantec Drive Encryption users will use when they shred. The default is 3. The larger the number, the more secure the shred, but the longer the shred process takes.

- **Warn user before shredding files.** When selected, your Symantec Drive Encryption users will be warned before files on their system are shredded. Deselect to suppress this warning.

- **Automatically shred when emptying the Recycle Bin/Trash.** When selected, your Symantec Drive Encryption users will have files they delete from their system shredded instead of just deleted. Deselect to prevent deleted files from being shredded.

### File Share Tab

The fields on the File Share tab control settings for Symantec File Share Encryption. For detailed descriptions of these settings, see the *Symantec Encryption Management Server Administrator's Guide.*

The fields on the File Share tab are:

- **Symantec File Share Encryption for Windows.** Deselect to disable the Symantec File Share Encryption feature; it will not appear in the user interface. Does not apply to Symantec Drive Encryption users.

- **Allow the user to create Symantec File Share Encryption folders.** Does not apply to Symantec Drive Encryption users.

- **Allow the user to enable Advanced User Mode.** Does not apply to Symantec Drive Encryption users.

- **Force the encryption of files in the following folders.** Does not apply to Symantec Drive Encryption users.
- **Prevent the encryption of files in the following folders.** Does not apply to Symantec Drive Encryption users.
- **Force the encryption of files associated with the following applications.** Does not apply to Symantec Drive Encryption users.
- **Prevent the automatic decryption of files by the following applications.** Does not apply to Symantec Drive Encryption users.

**Drive Encryption Tab**

The fields on the Drive Encryption tab control settings for PGP Virtual Disk and Symantec Drive Encryption.

---

**Note:** There are a few features of Symantec Drive Encryption that are supported on Windows systems but not on Mac OS X or Linux systems. If you configure these features for your Windows clients and also create Mac OS X and/or Linux clients, the settings for these features will be ignored on the Mac OS X and Linux systems; all other settings will work normally.

---

The fields on the Drive Encryption tab are:

- **PGP Virtual Disk.** Deselect to disable the PGP Virtual Disk feature; it will not appear in the user interface and it will not be available to your users.
- **Automatically create PGP Virtual Disk on Windows clients upon installation.** When selected, a PGP Virtual Disk volume will be created automatically for your Symantec Drive Encryption users using the Capacity and Format you specify.
- **Unmount when inactive for X minutes.** When selected, the PGP Virtual Disk volumes of your Symantec Drive Encryption users will be automatically unmounted after the specified number of minutes of inactivity on their systems. This could prevent the protected data on a PGP Virtual Disk volume from being available to unauthorized persons if you leave work without unmounting the volume, for example. Deselect to prevent PGP Virtual Disk volumes from being automatically unmounted because of inactivity.
- **Unmount on system sleep.** When selected, the PGP Virtual Disk volumes of your Symantec Drive Encryption users will automatically unmount if the system goes to sleep. Some systems do not support sleep mode, so this option would not apply. Deselect to prevent unmount on sleep.
- **Prevent sleep if disk(s) cannot be unmounted.** When selected, the systems of your Symantec Drive Encryption users will not sleep if, for some reason, a PGP Virtual Disk volume cannot be unmounted. Using this option could prevent loss of data. Deselect to permit sleep even if a volume cannot be unmounted.
- **PGP Portable.** Deselect to prevent your Symantec Drive Encryption users from creating PGP Portable disks. Enable to allow this. PGP Portable requires a separate license.
- **Symantec Drive Encryption.** Deselect to disable the Symantec Drive Encryption feature; it will not appear in the user interface. If you want your users to be able to use the Symantec Drive Encryption feature, do not deselect this field.
- **User-Initiated Drive Encryption Permissions.** Specify which encryption tasks your Symantec Drive Encryption users can do with internal and removable disks:
- **Allow User Management.** Your Symantec Drive Encryption users can add or remove other passphrase users from the user’s device.

- **Allow Encryption.** Your Symantec Drive Encryption users can initiate encryption of internal and/or removable disks. Automatic disk encryption during setup is not affected by this policy.

- **Allow Decryption.** Your Symantec Drive Encryption users can initiate decryption of internal and/or removable disks. If you do not enable this option, users will not be able to decrypt disks. Decryption after license expiration is not affected by this policy.

- **Store decryption policy on fixed disks.** When selected, the policy that specifies whether users can initiate decryption of the disk is stored on the encrypted disk. When the policy is stored on the disk, current and future versions of Symantec Drive Encryption, as well as Windows PE tools and other recovery methods, will all be prevented from decrypting the disk. This information is not stored on removable disks.

- **Allow/Deny/Force encryption of disks to existing Windows Single Sign-On password.** When selected, you can decide to Allow, Deny, or Force the use of the Single Sign-On (SSO) feature of Symantec Drive Encryption, which lets your users log into Symantec Drive Encryption and Windows at the same time. Deselect to prevent your users from using the single sign-on feature of Symantec Drive Encryption. **Allow** lets your users decide whether or not to use SSO, **Deny** prevents them from using it, **Force** requires them to use it. The SSO feature is only available for Windows clients.

  **Note:** Using the Single Sign-On feature is both a popular feature and it can be leveraged to enforce Symantec Drive Encryption passphrase quality alignment with your corporate passphrase quality requirements.

- **Automatically encrypt <volume type> at installation.** When selected, forces whole disk encryption of the boot disk, only the boot partition, or only the Windows partition when Symantec Drive Encryption is installed. Deselect to disable this feature.

- **Require <authentication method>.** When selected, you must specify a **required** method for securing the whole disk encrypted drive. This option is active only if **Automatically encrypt Boot disk at installation** is selected.

  The three security methods available are:

  - **standard passphrase authentication:** Requires that standard passphrase authentication be used to secure the drive. This is the default setting.

  - **supported smart cards for hardware security:** Requires that a supported smart card be used to secure the drive. The drive cannot not be whole disk encrypted until a supported smart card is provided; for example, an Aladdin eToken. The smart card must be configured before attempting to use it to secure a drive and the system must **already** have the appropriate drivers installed. Keys created on smart cards and tokens are **not** compatible with Symantec Drive Encryption’s key reconstruction feature.

  - **Trusted Platform Module (TPM):** Requires that a system with a hardware TPM be used to secure the drive. The drive will not be whole disk encrypted unless a hardware TPM is present.
- **Force maximum CPU Usage.** When selected, makes the process of whole disk encrypting a drive faster by using more CPU cycles. Deselect to prevent extra CPU cycles from going to the whole disk encryption process. Some systems may experience lag during usage when Maximum CPU Usage is enabled. You can only select this option if **Automatically encrypt Boot disk at installation** is selected.

- **Force power failure safety.** When selected, in the event of a power failure during whole disk encryption of a drive, the system can recover the data and restart encryption. Deselect to disable this feature. Initial encryption may take longer when Power failure safety is enabled. You can only select this option if **Automatically encrypt Boot disk at installation** is selected.

- **Lock passphrase user accounts on Windows clients after 3 failed login attempts.** Specify how many failed login attempts can occur before the encrypted disk is locked.

  If the disk is locked, all passphrase users lose access. All accounts on the disk are locked. Users will not be able to log in again without using a WDRT or other token. An administrator with a Symantec Drive Encryption administrator key can also unlock the account. If one user logs in with a WDRT or other token, the disk unlocks and all passphrase users can log in again. Without a WDRT or other token, the disk is permanently locked.

- **Enable automatic encryption or locking of removable devices.** If you select this option, the Automatic Encryption dialog box appears when the user inserts an unencrypted removable disk. The Automatic Encryption dialog box warns the user that the disk will be either mounted read-only, or encrypted after the amount of time you specify. This prevents protected data from being copied onto an unprotected drive.

  This feature is only available for Windows clients. Refer to the *Symantec Encryption Desktop for Windows User's Guide* for more information.

  - **Lock device as read-only and provide users with the option to encrypt with Symantec Drive Encryption (Windows clients only).** If you select this option, the unencrypted disk is mounted read-only. Users can read the data on the disk, but cannot save anything to the disk. Users can choose to encrypt the disk instead.

  - **Encrypt with Symantec Drive Encryption on Windows clients: After 30 seconds, After 1 minute, After 2 minutes, After 5 minutes, Immediately.**

  A dialog box displays a countdown until the device is encrypted. Removable drives on the system are encrypted after the dialog times out.

  By default, Symantec Encryption Desktop encrypts the drive to the existing credentials if the primary computer disk is encrypted. If the primary computer disk is not encrypted, Symantec Encryption Desktop will try to encrypt the portable drive to another private key, if one is available. If there is no other private key, the user will be prompted to create a passphrase user account to use to encrypt the disk.

  If a Whole Disk Recovery Token is required for encryption, then if the user attaches a previously unencrypted removable drive to the client computer while the Symantec Encryption Management Server cannot be reached, the removable disk cannot be encrypted and will be automatically unmounted. The removable disk cannot be used and the user will see the following error message: “The administrative server is not available for storing the administrative recovery token. Disk encryption cannot continue.”
- **Enable Whole Disk Recovery Tokens.** When selected, Symantec Drive Encryption administrators can remotely regain access to a drive that has been whole disk encrypted if the usual authentication method is unavailable (for example, if a user forgets their passphrase). Deselect to disable this option.

- **Allow configuration of Drive Encryption Local Self Recovery for Windows clients.** When selected, provides a way for users to access encrypted drives from the PGP BootGuard login screen if they have forgotten their passphrases. Users can log in by answering security questions they have previously configured. When configured, users will not have to contact an administrator for assistance.

  **Note:** This setting also applies to Linux clients.

- **Display a list of users who are eligible for local self recovery at boot time.** When selected, Symantec Drive Encryption displays a list of all users on that computer who have configured Local Self Recovery.

- **Encrypt using AES-256/AES-128.** AES-256 is stronger, but requires PGP Desktop 10 or greater clients.

- **Encrypt Windows Drive Encryption disks and PGP Virtual Disks to a Disk Administrator Key.** When selected, lets you add a public key which, if your users whole disk encrypt a drive, will be used to create a token-based user on the drive. Deselect to disable this option. This gives you a way to access the data on a whole disk encrypted drive or decrypt the drive if the user is unable or unwilling. To import the public key, click **Import** and do one of the following:
  - Select **Import Public Key File**, use the **Browse** button to navigate to the file of the public key you are importing (use Symantec Encryption Desktop to create this file if it does not already exist), select the file, click **Open**, then click **Import**.
  - Select **Import Public Key Block**, then paste the key block of the public key you are importing, then click **Import**.

  To access the whole disk encrypted drive via the token-based user, the private key must be on a supported token/smart card. Use Symantec Encryption Desktop to either create a keypair on or copy a keypair to a supported token/smart card. Refer to the **Symantec Encryption Desktop User's Guide** for more information about PGP keys and tokens/smart cards.

- **Encrypt Drive Encryption disks to a Disk Administrator Passphrase.** When selected, lets you add a passphrase that permits a Symantec Drive Encryption administrator to log in at the PGP BootGuard screen; for example, to create an account on an encrypted disk for a new user. Does not require a hardware token. This feature does not support Single Sign-On. Click **Create** to create a passphrase.

- **Display simple authentication field.** Select if you want only a single authentication field to appear on the PGP BootGuard screen of your Symantec Drive Encryption users.

- **Display detailed authentication fields.** Select if you want detailed authentication fields to appear on the PGP BootGuard screen of your Symantec Drive Encryption users. Refer to the Symantec Encryption Management Server online help for detailed information.

- **Add additional text to the Encryption BootGuard login screen.** When selected, lets you put in text that your users will see when the PGP BootGuard login screen appears on their system. You can use one line of text, up to 80 characters (including spaces). Deselect to disable this option.
- **Customize screen backgrounds.** When selected, lets you add custom background images that your users will see when the PGP BootGuard screen appears on their system or choose a plain gray background. You can add an image for both the splash and the login screen. Deselect to disable this option.
  - To add a background image, select **Upload background image files**, then click **Browse** next to either **Splash Screen** or **Login Screen** and select an image for one or both.
  - To display a plain gray background, select **Display plain gray background**.

The custom background images must be created according to the following specifications:
- XPM files only.
- Image size of 640 by 480.
- Palette of 15 colors only, *including black* (one color is reserved for fonts). You do not have to use all 15 colors in the image.
- 8-bit RGB only (cannot be 16-bit RGB). You can verify this by looking at the XPM header using a text editor: 8-bit values appear as #285A83 (one hex triplet), 16-bit values appear as #28285A5A8383 (two hex triplets).

Graphics applications that support the XPM file format include GIMP on Mac OS X/FreeBSD and UNIX/Linux, the Convert command on Linux, and Graphic Converter on Mac OS X.

For more information about creating custom background images for the PGP BootGuard screen, refer to the Symantec Encryption Management Server online help.

- **Enable audio cues.** When selected, enables the use of audio clues for certain actions that occur during the PGP Bootguard authentication process. These audio clues can help vision-impaired users more easily navigate the PGP BootGuard process. Deselect to disable this option.

If a user changes this setting, they must reboot their system to have the change take effect.

When enabled, the user's system will play audible tone combinations during the PGP BootGuard authentication process. Each tone combination starts with a middle sound and is followed by either a higher tone, another middle tone, or a lower tone. The three combinations are:
- Ready for passphrase/pin entry: When the system is first ready for passphrase/pin entry, the middle-middle tone combination plays, indicating the user can enter their passphrase or pin.
- Successful authentication: If the authentication attempt was successful, the middle-high tone combination plays, indicating success. The system then continues booting.
- Unsuccessful authentication: If the authentication attempt was unsuccessful, the middle-low tone combination plays, indicating failure. The BootGuard authentication screen displays and the passphrase field is cleared for another authentication attempt.

The tone combinations cannot be customized; you can only decide whether to enable or disable them.
Licensing Settings

On the Client Licensing screen (Consumers > Consumer Policy > Symantec Encryption Desktop > Client Licensing), the licensed features are shown, grouped by PGP Desktop versions newer than 9.5 and PGP Desktop version 9.0. These license settings are integrated into the client installers. The Licensee Count is updated dynamically as users enroll.

- **Licensee Name:** The name of the person under which the licenses were purchased.
- **Licensee Organization:** The name of the organization that purchased the licenses.
- **Licensee Email:** The email address of the person to contact regarding the license.
- **Options:** The Symantec Encryption Desktop features that can be enabled based on this license.
- **Licensee Count:** The number of consumers currently using this license.
Creating the Symantec Drive Encryption Client Installer

Once you have configured the settings for your Symantec Drive Encryption client installers, there are three ways to actually create the Symantec Drive Encryption client installer:

- With auto-detect policy
- With preset policy
- With no policy settings

In This Chapter

Creating an Installer with Auto-Detect Policy .......................................................... 45
Creating an Installer with Preset Policy ................................................................. 46
Creating an Installer with No Policy Settings ....................................................... 47

Creating an Installer with Auto-Detect Policy

This option for creating your Symantec Drive Encryption client installers uses your organization’s LDAP directory and requires that the LDAP Directory Synchronization feature already be enabled and appropriately configured on the Symantec Encryption Management Server.

To create a Symantec Encryption Desktop installer with auto-detect policy

1. Create the custom user policies you want to be linked to your Symantec Drive Encryption users. If you do not create any custom user policies, then your Symantec Drive Encryption users will automatically be linked to the default policy. You can, however, create custom user policies in the future that may be linked to your Symantec Drive Encryption users, depending on the settings in the custom policies.

2. Configure and save the settings on the Symantec Encryption Desktop screen appropriately for these custom user policies. Refer to your Symantec Encryption Management Server Administrator’s Guide for specific instructions.

3. Navigate to Consumers > Groups, then click Download Client. The Download Symantec Encryption Desktop Client page appears.

4. In the Client field, select Symantec Encryption Desktop.

5. In the Platform field, select Mac OS X, Linux 32-bit, Linux 64-bit, Windows 32-bit, or Windows 64-bit, as appropriate.

6. In the Language field, select English, French, German, Japanese, or Spanish, as appropriate.
Creating an Installer with Preset Policy

This option for creating your Symantec Drive Encryption client installers does not use an LDAP directory nor the LDAP Directory Synchronization feature.

To create a Symantec Drive Encryption client installer with preset policy

1. Create the custom user policy you want to be linked to your Symantec Drive Encryption users. If you do not create a custom user policy, then the Internal Users: Default policy will be the only policy with which you can link your Symantec Drive Encryption users.

2. Configure the settings on the Symantec Encryption Desktop screen appropriately for the custom user policy.

3. Navigate to Consumers > Groups, then click Download Client. The Download Symantec Encryption Desktop Client page appears.

4. In the Client field, select Symantec Encryption Desktop.

5. In the Platform field, select Mac OS X, Linux 32-bit, Linux 64-bit, Windows 32-bit, or Windows 64-bit, as appropriate.

6. In the Language field, select English, French, German, Japanese, or Spanish, as appropriate.

7. Make sure the Customize checkbox is selected. If it is not selected, select it.

8. Select Preset Policy Group.
Creating an Installer with No Policy Settings

You have the option of creating your Symantec Drive Encryption client installer with no policy settings, which means that your Symantec Drive Encryption users can do anything their license allows; they will not receive any policies from the Symantec Encryption Management Server. Note that this option is virtually the same as standalone usage, and defeats the purpose of using a Symantec Encryption Management Server to manage your Symantec Drive Encryption users.

To create a Symantec Encryption Desktop installer with no associated policy

1. Navigate to Consumers > Groups, then click Download Client. The Download Symantec Encryption Desktop Client page appears.
2. In the Client field, select Symantec Encryption Desktop.
3. In the Platform field, select Mac OS X, Linux 32-bit, Linux 64-bit, Windows 32-bit, or Windows 64-bit, as appropriate.
4. In the Language field, select English, French, German, Japanese, or Spanish, as appropriate.
5. Make sure the Customize checkbox is deselected. If it is selected, deselect it.
6 Click **Download**. The Symantec Encryption Desktop installer is created and downloaded to your system.
Controlling Symantec Drive Encryption Components

One of the ways you can control what your users can do with Symantec Drive Encryption is by disabling specific Symantec Drive Encryption components. This is accomplished by using software to distribute your client installers that has the ability to specify switches to the msiexec.exe command line utility.

**Note:** This feature is available for Windows clients only.

Disabling a Symantec Drive Encryption component means it will not appear in the Symantec Drive Encryption user interface, and it ensures that there will not be any compatibility issues with the operating system or third-party products.

Upgrades, including automatic upgrades, honor the disabling of Symantec Drive Encryption components and will not re-enable disabled components unless the MSI file has been specifically edited to re-enable the disabled component.

The table lists the Symantec Drive Encryption components that can be disabled and the effects of disablement.

<table>
<thead>
<tr>
<th>Component</th>
<th>What Gets Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>GROUPWISE</td>
<td>Groupwise messaging.</td>
</tr>
<tr>
<td>LSP</td>
<td>The IM encryption feature and SMTP, POP, and IMAP messages.</td>
</tr>
<tr>
<td>MAPI</td>
<td>MAPI messaging.</td>
</tr>
<tr>
<td>MEMLOCK</td>
<td>The memory locking feature that keeps sensitive data from leaving volatile memory. Disabling memory lock is available so that you can disable all kernel-level items, if desired. It should generally <strong>not</strong> be disabled unless you have a specific reason to do so.</td>
</tr>
<tr>
<td>NETSHARE</td>
<td>The Symantec File Share Encryption feature.</td>
</tr>
<tr>
<td>NOTES</td>
<td>Notes messaging.</td>
</tr>
<tr>
<td>SSO</td>
<td>The Symantec Drive Encryption Single Sign-On feature.</td>
</tr>
<tr>
<td>VDISK</td>
<td>The PGP Virtual Disk feature.</td>
</tr>
<tr>
<td>WDE</td>
<td>The Symantec Drive Encryption feature.</td>
</tr>
</tbody>
</table>

The syntax to disable Symantec Encryption Desktop components is:

```bash
> msiexec /I pgdesktop.msi PGP_INSTALL_[component]=0
```

Where `[component]` is the Symantec Encryption Desktop component you want to disable.

You can disable multiple Symantec Encryption Desktop components using a single command. For example:
To re-enable a Symantec Encryption Desktop component that was disabled requires a
reinstallation with the disabled component specifically re-enabled. For example:

```bash
> msiexec /I pgpdesktop.msi PGP_INSTALL_MAPI=1
```
Testing the Symantec Drive Encryption Client Installer

Once you have created a Symantec Drive Encryption client installer with the desired settings for your Symantec Drive Encryption users, Symantec Corporation strongly recommends that you not immediately deploy it. Instead, test your client installer on as many representative machines as you can; you will save yourself a lot of time by finding and solving problems with the installer before your full deployment.

Naturally, if any of these tests have unexpected results, you will need to fix the problems and, if necessary, create an updated client installer.

Ways of testing your Symantec Drive Encryption client installer include:

- Install it on a network that is separate from your production environment.
- Install it on a system configured with your standard corporate image.
- Install it on a system with your standard corporate image plus other software common in your organization, allowed or not.
- Run a pilot deployment to a small number of users or a single department.
Deploying the Symantec Drive Encryption Client Installer

How you deploy the Symantec Drive Encryption client installer to your users depends on your unique circumstances. Note that the Symantec Encryption Management Server, which manages your Symantec Drive Encryption clients, cannot be used to deploy the client installer.

Some common methods include:

- Using an enterprise software distribution system such as SMS or Tivoli
- Downloading from a Web/file server
- Distributing on a CD, DVD, or thumb drive

If you want to control Symantec Drive Encryption components during deployment (see *Controlling Symantec Drive Encryption Components* (on page 49)), make sure the deployment software you plan to use has the ability to specify switches to the msiexec.exe command line utility.
Assisting Your Symantec Drive Encryption Users

There are a number of things that Symantec Corporation recommends you do to help support your Symantec Drive Encryption users:

- Provide your Symantec Drive Encryption users with a document, created by your organization, that talks about Symantec Drive Encryption: this document could include what Symantec Drive Encryption is, what they are expected to use it for, what it does to their system, and what to do if they have problems with Symantec Drive Encryption. For more information about what information you could include in such a document, refer to The End-User Experience (on page 57).

- Even if you do not provide your Symantec Drive Encryption users with a document that talks about Symantec Drive Encryption, you should definitely give them a written statement about what Symantec Drive Encryption should be used for and what it must be used for. Include a summary of your official corporate security policies and how they can use Symantec Drive Encryption to conform to those policies.

- Give them a copy of the Symantec Drive Encryption Quick Start Guide and the Symantec Encryption Desktop User's Guide. Strongly encourage them to read the Quick Start Guide before installing Symantec Drive Encryption on their systems.

  **Note:** To view the most recent version of these documents, go to the Symantec Corporation Support website (http://www.symantec.com/business/support/).

- Tell them about the other resources that are available to them, including the built-in online help.

- Tell them about steps they should take to make sure their drives are in good condition before they whole disk encrypt them, especially checking the drive for errors. Symantec Corporation recommends a third-party scandisk utility such as SpinRite or Norton Disk Doctor, for example. Tell them that defragmenting the drive is also a good idea; recommend the built-in Windows utility or a third-party utility, such as PerfectDisk.

- Give them help desk contact information within your organization, in case they experience problems.

- Set up a system so that each user can report a successful installation.
The End-User Experience

Your Symantec Drive Encryption users will notice changes to how they use their computer both during the installation of Symantec Drive Encryption and afterwards. You can help ensure a successful end-user experience with Symantec Drive Encryption by preparing your end users for these changes.

If you decide to provide your Symantec Drive Encryption users with a document created by your organization, you may want to include some or all of the following points.

Depending on configuration, some of these points may not apply to your Symantec Drive Encryption users.

In This Chapter

During the Installation Process .................................................................57
During Symantec Drive Encryption Setup .....................................................58
During Normal Usage ...................................................................................58

During the Installation Process

The following items may impact your Symantec Drive Encryption users during installation:

- The installation process begins by double-clicking the Symantec Drive Encryption client installer. A reboot of the system is required when the installation process is complete.

- During the installation process, Symantec Drive Encryption will coordinate with the Symantec Encryption Management Server and link to the most appropriate user policy. This linkage is based on how closely the settings for the particular user in the LDAP directory match the settings of the available user policies (if LDAP Directory Synchronization is being used). If you later add a more appropriate policy, the affected Symantec Drive Encryption users will automatically become linked to the new, more appropriate policy. Note that the MSIE proxy setting of the user must be correct if they are enrolling from outside your corporate network.

- Unless Server Key Mode is the only allowed key mode, the installation process will prompt your Symantec Drive Encryption users to create a PGP keypair. If you are allowing them to select between two or more keys modes, you should provide them with guidance regarding what is the best choice based on how they will be using the product.

- If you are not using encrypted email, have your Symantec Drive Encryption users leave the email field blank when they are creating their PGP keypair and have them skip adding their public key to the PGP Global Directory. This will ensure that they do not get encrypted email they cannot decrypt.
Part of the installation process includes a "cookie" being placed onto the systems of your Symantec Drive Encryption users. This is required for communications between the system and the Symantec Encryption Management Server.

## During Symantec Drive Encryption Setup

The following items may impact your Symantec Drive Encryption users during setup:

- You can configure whole disk encryption of the boot drive on the systems of your Symantec Drive Encryption users to begin automatically or you can let them start the process manually sometime after installation.
- Whole disk encryption of a drive is a background process; your Symantec Drive Encryption users can continue to use their systems while the drive is being encrypted.
- The process of whole disk encrypting a drive can be paused, either manually or if the system is shut down or restarted, goes into standby mode, or on laptops if the system goes to battery power (you can only begin whole disk encrypting a drive on a laptop if the system is on AC power).
- On rare occasions, the whole disk encryption of a drive stops and displays the "Unable to instrument disk" error message. This usually occurs when there is not enough contiguous space available on the drive being encrypted, there are disk errors on the drive, or if Windows is reserving some of the space being used to encrypt the drive. The solution is to have the user check the drive for errors and defragment it, then try again to whole disk encrypt it.

## During Normal Usage

The following items may impact your Symantec Drive Encryption users during usage:

- On startup, the PGP Bootguard screen will appear, requiring appropriate authentication before allowing access to data on the system.
- The PGP Tray icon will appear in the Windows System Tray (on Windows systems), providing easy access to many Symantec Drive Encryption features.
- The Notifier screen will appear when Symantec Drive Encryption performs certain actions, providing information about the action being taken.
- Symantec Drive Encryption functionality may change from time to time if the policies change that apply to a user. Symantec Drive Encryption checks with the Symantec Encryption Management Server it is enrolled with for policy changes at startup, every 24 hours after startup, when email messages are sent (if email proxying is enabled).