Symantec™ Drive Encryption

Deployment Guide

10.3
# Contents

<table>
<thead>
<tr>
<th>Overview</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audience</td>
<td>3</td>
</tr>
<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>7</td>
</tr>
<tr>
<td>Support agreement resources</td>
<td>7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Understanding Symantec Drive Encryption</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Symantec Drive Encryption</td>
<td>9</td>
</tr>
<tr>
<td>Components of a Typical Symantec Drive Encryption Deployment</td>
<td>10</td>
</tr>
<tr>
<td>How Symantec Drive Encryption Works</td>
<td>10</td>
</tr>
<tr>
<td>About Symantec Encryption Management Server</td>
<td>11</td>
</tr>
</tbody>
</table>

| Major Steps | 13 |

<table>
<thead>
<tr>
<th>Preparation</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Test Environment</td>
<td>15</td>
</tr>
<tr>
<td>Placing the Symantec Encryption Management Server in your Network</td>
<td>16</td>
</tr>
<tr>
<td>Adding the Symantec Encryption Management Server to your Network</td>
<td>16</td>
</tr>
<tr>
<td>Deployment Options</td>
<td>17</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>19</td>
</tr>
<tr>
<td>Understanding the LDAP Directory Synchronization Feature</td>
<td>19</td>
</tr>
<tr>
<td>Understanding Policies</td>
<td>20</td>
</tr>
<tr>
<td>Preparing User Systems</td>
<td>20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Installation and Configuration</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before You Install</td>
<td>23</td>
</tr>
<tr>
<td>Installing the Server Software</td>
<td>24</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuring the Symantec Encryption Management Server</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removing Unneeded Services</td>
<td>27</td>
</tr>
<tr>
<td>Setting Up Administrators</td>
<td>28</td>
</tr>
<tr>
<td>Establishing Backups</td>
<td>28</td>
</tr>
<tr>
<td>Securing your Symantec Encryption Management Server</td>
<td>29</td>
</tr>
<tr>
<td>Configuring Policies</td>
<td>30</td>
</tr>
<tr>
<td>Configuring the LDAP Directory Synchronization Feature</td>
<td>30</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Enrollment</td>
<td>31</td>
</tr>
<tr>
<td>Email Enrollment</td>
<td>32</td>
</tr>
<tr>
<td>LDAP Directory Synchronization Enrollment</td>
<td>32</td>
</tr>
<tr>
<td>Backing Up Your System</td>
<td>33</td>
</tr>
<tr>
<td>Establishing Symantec Drive Encryption Client Settings</td>
<td>35</td>
</tr>
<tr>
<td>General Settings</td>
<td>35</td>
</tr>
<tr>
<td>Consumer Policy Options General Page – Best Practices</td>
<td>36</td>
</tr>
<tr>
<td>Consumer Policy Options General Page – Settings</td>
<td>36</td>
</tr>
<tr>
<td>Key Settings</td>
<td>37</td>
</tr>
<tr>
<td>Key Generation Settings</td>
<td>37</td>
</tr>
<tr>
<td>Key Mode Settings</td>
<td>38</td>
</tr>
<tr>
<td>Certificates Settings</td>
<td>39</td>
</tr>
<tr>
<td>Options Settings</td>
<td>41</td>
</tr>
<tr>
<td>Symantec Encryption Desktop Settings</td>
<td>42</td>
</tr>
<tr>
<td>General Tab – Best Practices</td>
<td>43</td>
</tr>
<tr>
<td>General Tab – Settings</td>
<td>43</td>
</tr>
<tr>
<td>Messaging &amp; Keys Tab</td>
<td>46</td>
</tr>
<tr>
<td>Zip &amp; Shredder Tab</td>
<td>48</td>
</tr>
<tr>
<td>File Share Tab</td>
<td>49</td>
</tr>
<tr>
<td>Drive Encryption Tab – Best Practices</td>
<td>50</td>
</tr>
<tr>
<td>Drive Encryption Tab – Settings</td>
<td>51</td>
</tr>
<tr>
<td>Licensing Settings</td>
<td>58</td>
</tr>
<tr>
<td>Creating the Symantec Drive Encryption Client Installer</td>
<td>59</td>
</tr>
<tr>
<td>Creating an Installer with Auto-Detect Policy</td>
<td>59</td>
</tr>
<tr>
<td>Creating an Installer with Preset Policy</td>
<td>60</td>
</tr>
<tr>
<td>Creating an Installer with No Policy Settings</td>
<td>61</td>
</tr>
<tr>
<td>Controlling Symantec Drive Encryption Components</td>
<td>63</td>
</tr>
<tr>
<td>Testing the Symantec Drive Encryption Client Installer</td>
<td>65</td>
</tr>
<tr>
<td>Deploying the Symantec Drive Encryption Client Installer</td>
<td>67</td>
</tr>
<tr>
<td>Assisting Your Symantec Drive Encryption Users</td>
<td>69</td>
</tr>
<tr>
<td>The User Experience</td>
<td>71</td>
</tr>
<tr>
<td>During the Installation Process</td>
<td>71</td>
</tr>
<tr>
<td>During Symantec Drive Encryption Setup</td>
<td>72</td>
</tr>
<tr>
<td>During Normal Usage</td>
<td>72</td>
</tr>
</tbody>
</table>
1

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

Audience

The audience for this guide is an IT or support professional who is involved in 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 users for a successful installation.

Before you use this guide, read the Symantec Encryption Management Server Administrator's Guide, and install and use a Symantec Encryption Management Server.

Symantec recommends that you take the time to understand how you plan to use the software products available from Symantec Corporation, now and later. The decisions that you make now in deploying Symantec Drive Encryption—for example, your choice of key mode—affect how you can do things in the future.

Symantec also recommends that you create a test environment to verify that your setup meets your requirements before you deploy it into a production environment.

Note: Back up your data to avoid data loss. Symantec is not responsible for any data loss or system recovery.

Before you deploy Symantec Drive Encryption, create a centralized backup solution. For additional information on deployment best practices and drive compatibility, see the knowledge base article Best Practices: Symantec Drive Encryption at http://www.symantec.com/docs/TECH149543.
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 plan to use as a management console. Specifically, the guide describes how to configure your Symantec Encryption Management Server, using the server to establish settings for your Symantec Drive Encryption clients, and create 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 describes the features of the Symantec Drive Encryption product. Consider distributing the Symantec Drive Encryption QSG to your 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. For 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**
  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
Overview

Technical Support

- 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 can access Technical Support information at the following URL:

www.symantec.com/business/support/

Before you contact Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. In addition, 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
- Msiinfo file
- 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
2

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 boot disk encryption. Symantec Drive Encryption on Linux systems has a command-line interface and supporting the drive 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. Note that drive encryption is only one feature of the Symantec Drive Encryption product on Windows and Mac OS X systems. Linux systems only support the drive encryption 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 Symantec Drive Encryption Works

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

1. **Encrypt the boot drive on the system.**
   
   Automatically or manually, the Symantec Drive Encryption passphrase or token (Windows systems only) user encrypts the boot drive on their system. Symantec Drive Encryption transparently encrypts the drive sector by physical sector.

2. **Authenticate on the PGP BootGuard screen.**
   
   Once encryption begins, and thereafter, the Symantec Drive Encryption user must authenticate using the PGP BootGuard screen.
3 Use Passphrase or USB token (Windows systems only) to access the system.
   To access the system, the Symantec Drive Encryption user types a passphrase or
   inserts their USB token to authenticate.

4 Log in to Microsoft Windows (Windows systems only)
   If you enabled the Single Sign-On feature, after the Symantec Drive Encryption
   users authenticate on the PGP BootGuard screen, they are automatically logged in
   to Microsoft Windows.
   A Symantec Drive Encryption user’s system behaves as it did before encryption.

About Symantec Encryption Management Server

Symantec Encryption Management Server is the platform that you use to manage and
deploy Symantec Drive Encryption. You use it to configure client options and to provide
them with custom policies and settings. You also use Encryption Management Server to
create the client installers and manage them after installation. For example, you use
Encryption Management Server to provide Whole Disk Recovery Tokens for each of
your managed clients.

You can use Symantec Encryption Management Server to provide your enterprise with
secure messaging by transparently protecting your messages without user interaction.
The Symantec Encryption Management Server encrypts, decrypts, signs, verifies
messages, and provides strong security through policies that you control.
The information in this guide is organized into major steps. These steps are in the order that Symantec Corporation recommends you use to deploy Symantec Drive Encryption. Depending on your environment, you may need to perform some of these tasks within the steps in a slightly different order.

Follow these steps to configure and deploy Symantec Drive Encryption clients using a Symantec Encryption Management Server as the management console:

1 **Preparation**
   Describes what you must do to prepare you environment for your Symantec Encryption Management Server installation:
   - Create a test environment to use to practice installing, configuring, deploying, and using Symantec Drive Encryption.
   - Locate your Symantec Encryption Management Server in your network.
   - Add the Symantec Encryption Management Server to your network.
   - Configure your firewall to support the Symantec Encryption Management Server.
   - Select the enrollment method that you want your Symantec Drive Encryption users to use.
   - Set up LDAP directory synchronization (if applicable).
   - Verify that the disk is compatible with Symantec Drive Encryption.
   - Create a backup of the data before encrypting the disk.

   See [Preparation](#) (on page 15).

2 **Installation and configuration**
   Describes the process to install and configure the Symantec Encryption Management Server software. All Symantec Encryption Management Server setups use this process, but there are some things specific to deployments.

   See [Installation and Configuration](#) (on page 23).

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

   See [Configuring the Symantec Encryption Management Server](#) (on page 27).
4 Setting Symantec Drive Encryption client options
   Describes the settings that you use to configure Symantec Drive Encryption to
   meet your security requirements.
   See Establishing Drive Encryption Client Settings (on page 35).

5 Creating the Symantec Drive Encryption client installer.
   Describes the process to create the actual client installer executable.
   See Creating the Symantec Drive Encryption Client Installer (on page 59).

6 Testing the client installer
   Describes the methods you can use to test your client installer before you deploy
   it.
   See Testing the Symantec Drive Encryption Client Installer (on page 65).

7 Deploying the client installer to Symantec Drive Encryption users.
   Describes the options you can use to deploy the client installer executable to your
   Symantec Drive Encryption users.
   See Deploying the Symantec Drive Encryption Client Installer (on page 67).

8 Assisting your Symantec Drive Encryption users.
   Describes what you can do to help prepare your Symantec Drive Encryption users
   for the new encryption software.
   See Assisting Your Symantec Drive Encryption Users (on page 69).
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................................................................ 19
Understanding the LDAP Directory Synchronization Feature .............................. 19
Understanding Policies ................................................................................................ 20
Preparing End-User Systems ....................................................................................... 20

Creating a Test Environment

Symantec Corporation recommends that you first create a test environment so that you can become familiar with how to install, configure, deploy, and use Symantec Drive Encryption before you roll it out to your production environment.

Make sure that your test environment includes the same hardware, Windows and Mac OS X systems, software products, and other items that are included in your production environment.

Next, follow the steps in this guide to deploy and configure Symantec Drive Encryption in your test environment. Take note of any problems that occur, your solutions, and workarounds.
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.

- Remove or disable unneeded services. See *Removing Unneeded Services* (on page 27).

- 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* (on page 17).
  - 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. In addition, the management console needs certain ports open on your firewall for a variety of purposes.

You should make changes to the firewall 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.

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 Enrollment

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

You can use the following methods to enroll your Symantec Drive Encryption users:

- **LDAP Directory Synchronization Enrollment**
  To use this method, you must enable and correctly configure the LDAP Directory Synchronization feature. Then, in the Symantec Encryption Management Server’s management interface, on the Directory Synchronization page, select the Enroll clients using directory authentication check box.
  To enroll, the client authenticates to the LDAP directory that you specified in the LDAP Directory Synchronization feature.

- **Certificate Enrollment**
  When you enable clients to enroll with LDAP Directory Synchronization, you can enable the Symantec Drive Encryption users to use certificates or smart cards to enroll.
  To use this method, you must enable and configure Certificate Services on your Windows Server. In addition, Symantec Drive Encryption users also must be using smart cards or certificates to log in to Windows.

- **Email**
  To use this method, you must use SMTP email to set up communication between the Symantec Drive Encryption client and the Symantec Encryption Management Server. You can use this method with all client installations as long as the client system has a usable email account. You can use this method 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.

For more information on how to use LDAP directory synchronization enrollment and certificate enrollment, and email enrollment, see the topic Understanding User Enrollment Methods, in the Symantec Encryption Management Administrator’s Guide.

Understanding the Two Enrollment Paths

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

- If your organization has an up-to-date LDAP directory server, you may 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 your organization does not have an up-to-date LDAP directory server, keep the LDAP Directory Synchronization feature disabled, select Preset policy, and use email enrollment.

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 determines which users are in what groups for the purposes of applying the appropriate policy and for enrolling.

- **LDAP Directory Synchronization enabled, enrollment off**
  The specified LDAP directory determines which users are in what groups for the purposes of applying the appropriate policy, but not for enrollment purposes. Email enrollment is used for enrollment.
### Disabled

LDAP Directory Synchronization is disabled. The Symantec Encryption Management Server does not check any LDAP directories for users to be imported or for enrollment. Email enrollment is used for enrollment.

---

### 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 User Systems

Symantec Corporation recommends that you review the most recent version of the Symantec Encryption Desktop Release Notes, Symantec Drive Encryption Release Notes, and Symantec Encryption Management Server Release Notes to make sure that the systems in your deployment environment are ready for installation of both Symantec Encryption Management Server and Symantec Drive Encryption client.

As part of your installation preparation do the following:

- Verify your business requirements.

- Verify the hardware and the operating systems that you use in your environment.
  - Update your hardware and exempt the uncertified or old hardware.

  If you use Windows 8, see the knowledge base article Symantec Encryption Desktop 10.3.1 compatibility with Microsoft Windows 8 at [http://www.symantec.com/docs/TECH203071](http://www.symantec.com/docs/TECH203071).

  Note that Windows systems are more flexible than Mac OS X systems. For example, Mac OS X systems do not recognize all keyboards, and often a new Mac OS is no longer compatible with older versions of software.
- Verify that your hardware supports specific approved keyboards and smart cards.

  For more information about supported keyboards and smart cards, see the most recent version of the Symantec Encryption Management Server Release Notes, the Symantec Encryption Desktop User Guides, and the Symantec Encryption Management Server Administrator's Guide.

- Verify that your clients meet the listed minimum system requirements.

- Verify that you use supported email clients in your environment.

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

  For more information, see the most recent version of the Symantec Encryption Desktop Release Notes.

- Review the list of known software conflicts in the Additional Information section in the most recent version of the Symantec Encryption Desktop Release Notes to help you avoid these issues in your deployment.

- Verify that your client systems include scandisk and defragmentation software, so that they can prepare their drives for Symantec Drive Encryption installation.
  - Examples of scandisk software are Windows chkdsk.exe, SpinRite, or Norton Disk Doctor.
  - Examples of defragmentation software are Windows defrag.exe or PerfectDisk.

- Remove all non-Symantec encryption from your client systems.
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 ................................................................. 23  
Installing the Server Software .................................................. 24

---

**Before You Install**

Before you install the software:

- Have a centralized backup solution in place.
  
  Symantec Corporation recommends that before you implement Symantec Encryption Management Server and Symantec Drive Encryption into your system that you have a centralized backup solution in place. The backup solution helps to ensure that no data is permanently lost during installation or encryption.

- Back up your system

  Before you install, Symantec Encryption Management Server, Symantec Corporation recommends that you back up your system.

- Verify that you have certified hardware on which to install the Symantec Encryption Management Server software.

  To view the current list of certified hardware, see the *Symantec Encryption Management Server Certified Hardware List* section in the most recent version of the *Symantec Encryption Management Server Release Notes*.

- Acquire the most recent version of the Symantec Encryption Management Server software.

- Download the most recent version of the *Symantec Encryption Management Server Administrator’s Guide* and the *Symantec Encryption Management Server Installation Guide*.

Installing the Server Software

1. Back up your system.
   Before you install Symantec Encryption Management Server, Symantec Corporation recommends that you back up your system.

2. Do the default installation of the Symantec Encryption Management Server software.

3. After your default installation is complete, connect to the Symantec Encryption Management Server. Then, use the Setup Assistant to configure the server.
   To connect to the server, use the customnet, standard, ks, or expert installation option.
   For more information, see Configuring Symantec Encryption Management Server With the Setup Assistant in the Symantec Encryption Management Server Installation Guide.

4. On the Welcome page, read the text, and then click the Forward arrow to continue.

5. On the End User License Agreement page, read the text of the License Agreement, and then click I Agree.

6. On the Setup Type page, select New Installation, and then click the Forward arrow to continue.

7. On the Date & Time page, type or select the appropriate information, and then click the Forward arrow to continue.

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

9. On the Confirmation page, verify that the information is correct, and then click Done.
   The server reboots.

10. On the Licensing page, type or select the appropriate licensing information for the Symantec Encryption Management Server that you plan to use as a management console.
   
   **Note:** To configure and use mail proxies, select the Enable Mail Proxies check box.

11. Click Save.

12. On the Administrator Name & Passphrase page, type or select the appropriate information, and then click the Forward arrow to continue.

13. If on the Licensing page, you selected the Enable Mail Proxies check box, the Mail Processing page opens. Select Gateway Placement, and then click the Forward arrow to continue.

14. On the Mail Server Selection page, type or select the appropriate information, and then click the Forward arrow to continue.
15 On the **Ignition Keys** page, select the options that you want to use, and then click the **Forward** arrow to continue.

16 On the **Ignition Keys** page, type or select the appropriate information, and then click the **Forward** arrow to continue.

17 On the **Backup Organization Key** page, type a passphrase to protect your Organization Key, and then click **Backup Key**.

   An Organization Key is generated. This key allows you to restore your Symantec Encryption Management Server from a backup, should that be necessary.

   If you only use the Symantec Encryption Management Server as a management server, you cannot use the Organization Key to sign the keys that Symantec Encryption Management Server creates.

18 On the **Confirmation** page, verify that the settings are correct, and then click **Done**.
6

Configuring the Symantec Encryption Management Server

You need to configure multiple aspects of Symantec Encryption Management Server to prepare to use it as a management console:

- Remove unneeded services
- Set up administrators
- Establish settings for backups
- Secure the server
- Configure policies
- Configure the LDAP Directory Synchronization feature (if applicable)
- Configure enrollment
- Back up your system

In This Chapter

- Removing Unneeded Services ................................................................. 27
- Setting Up Administrators .................................................................. 28
- Establishing Backups ........................................................................... 28
- Securing your Symantec Encryption Management Server .................. 29
- Configuring Policies ............................................................................. 30
- Configuring the LDAP Directory Syncrhonization Feature ................. 30
- Configuring Enrollment ....................................................................... 31

---

Removing Unneeded Services

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

Do the following:

- Navigate to Mail > Proxies
  
  Delete the SMTP proxy; you do not need it.

- 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 accepts mail for delivery from the Symantec Encryption Management Server. This forces the Symantec Encryption Management Server not to use DNS for mail queries; instead, it sends all mail to the specified mail route.
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 check box 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 Corporation recommends that you establish a method for backing up your data. Once you establish a method, Symantec Corporation recommends that you back up your data often. For example, back up your data before installation and before encryption.

Symantec Encryption Management Server provides two methods to back up your data:

- Scheduled backups
- On-demand backups
Backup files can be stored on the Symantec Encryption Management Server. You can also use FTP or SCP to automatically send your backup files to a specified location.

**To establish automatic backups**

1. In the Symantec Encryption Server Administration console, on the System menu, click **Backups**.
2. On the System Backups page, click **Backup Schedule**.
3. In the Backup Schedule dialog box, select the Enable Scheduled Backups check box, if it is not already selected.
4. Select the check boxes for the days of the week on which you want your backups to be performed.
5. In the Start backups at drop-down lists, select a time for the backups to begin.
6. Click **Save**.

**To perform an on-demand backup**

1. In the Symantec Encryption Server Administration console, on the System menu, click **Backups**.
2. On the System Backups page, click **Backup Now**.
3. In the Individual Backup dialog box, in the Backup Name text box, type the name of your backup file. Then, click **Backup**.
   
   Your data is backed up immediately.
4. When the backup is complete, the backup file is displayed in the System Backup list.

For more information about backups, see *Backing Up and Restoring System and User Data* in 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 that your users can use to interact with the product. These settings include key settings, Symantec Drive Encryption client settings, directory services, client updates, and proxy server settings.

You can create and configure consumer policies to control which settings your Symantec Drive Encryption users can use. These consumer policies are different from the email policies that you can configure on the Symantec Encryption Management Server.

By default, one Symantec Drive Encryption user policy is always created, the Default policy.

To create and configure policies for your Symantec Drive Encryption users, you must first open the Consumer Policy page. In the Symantec Encryption Server Administration console, go to Consumers > Consumer Policy.

On the Consumer Policy page, you can do the following:

- Reconfigure the Default policy
  You may need to reconfigure the Default policy so that it conforms to your organization's security policies before you roll it out to your Symantec Drive Encryption users.

- Create Consumer policies
  Create and configure Consumer policies so that Symantec Drive Encryption conforms to your organization's security policies. Then roll the policies out to your Symantec Drive Encryption users.

  For example, if you require stronger security for executives or specific departments, you can create multiple internal user policies to support these security requirements.

To configure consumer policies, refer to Establishing Symantec Drive Encryption Client Settings (on page 35).

For more information about these settings, see Administering Consumer Policy in 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 policies 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

Two methods are available for enrollment:

- **Email (the default)**

  This enrollment method requires only the Symantec Drive Encryption client and the Symantec Encryption Management Server to use SMTP email to communicate. This method is available for all client installations that have 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 mail flow.

- **LDAP Directory Synchronization**

  This enrollment method requires you to enable and correctly configure the LDAP Directory Synchronization feature and to select the **Enroll clients using directory authentication** option on the **Directory Synchronization** page.

  To enroll, the client provides authentication credentials to the LDAP directory specified in the LDAP Directory Synchronization feature.

The following information is common to both enrollment methods:

- **Port 443** must be open between your Symantec Drive Encryption clients and the Symantec Encryption Management Server.
Symantec Drive Encryption clients use this port to get policy and receive encryption keys. Enrollment fails 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, 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 does not work because the domain does not exactly match what is configured on the Symantec Encryption Management Server.

You can configure multiple email domains on the Symantec Encryption Management Server. Configure eng.example.com as an additional domain to solve the problem.

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

**Email Enrollment**

To configure email enrollment:

- On your Symantec Encryption Management Server, go to Mail > Mail Routes and add a route from the protected domain to the hostname of your mail server.

  For example, 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 to 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.

- Make sure your mail server accepts SMTP.

  For example, Domino servers might not accept SMTP by default.

When your Symantec Drive Encryption users install Symantec Drive Encryption on their systems, an Enrollment Assistant appears, and asks 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**

Before you begin LDAP Directory Synchronization enrollment, make sure that user accounts, passwords, and domains are current and make sure to keep them current.

To perform 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. Tools such as these ensure that proper LDAP syntax is used during enrollment.
To use LDAP Directory Synchronization enrollment, your directory schema must contain specific attributes. For example, every user must have an email address in the attribute mail.

Other attributes to check include:
- cn, mail
- smtpProxyAddress (or proxyAddress SMTP:)
- uid
- sAMAccountName
- Usercertificate
- binary

These attributes (except Usercertificate and binary) and your LDAP filter attributes must be in the LDAP directory.

When your Symantec Drive Encryption users install Symantec Drive Encryption on their systems, they are prompted to authenticate (provide their username and password) to the LDAP directory. Make sure that they authenticate. Authentication is required for the successful completion of the enrollment process.

---

**Backing Up Your System**

After you configure the Symantec Encryption Management Server, Symantec Corporation recommends that you back up your system.

For more information about backing up your data, see *Establishing Backups* (on page 24).
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 ............................................................................................................ 35
Key Settings ................................................................................................................... 37
Symantec Encryption Desktop Settings .................................................................... 42
Licensing Settings......................................................................................................... 58

General Settings

These settings apply to client updates, proxy server, and Policy ADK options. The settings are found in the Symantec Encryption Management Server console (Consumers > Consumer Policy > [policy] > General > Edit).

The Consumer Policy Options page may differ, depending on if you are editing the Everyone group Consumer Policy or a policy that you created.
Consumer Policy Options General Page – Best Practices

As a best practice, Symantec recommends that you enable specific settings on the General page. These recommendations help keep your clients current. They also keep your clients and your Symantec Encryption Management Server product versions synchronized.

Recommended settings on the General page:

- **Notify users of software updates and automatically download**
  Select this option to keep the software on your client systems and Symantec Encryption Management Server up-to-date. In addition, select this option to keep client systems and Symantec Encryption Management Server synchronized with the same versions of the products that they have in common.

Consumer Policy Options General Page – Settings

The settings on the General page are:

- If you edit a user-created policy and you use LDAP Directory Synchronization enrollment, you can assign policies to internal users based on their directory attributes.
  
  For more information, see the *Symantec Encryption Management Server Administrator’s Guide*.

- **Notify users of software updates and automatically download**
  Select this option to keep the software on your client systems up-to-date.

- **Use an HTTPS Proxy Server for Symantec encryption client communications**
  Select this option if your Symantec Drive Encryption clients use a proxy server to connect to the Symantec Encryption Management Server.
  - **Hostname**
    Type the hostname of the HTTPS proxy server.
  - **Port**
    Type the port used to access the HTTPS proxy server.

- **Additional Decryption Key**
  Select this option to import a key to use as an Additional Decryption Key for this consumer policy.
  
  Click **Import** and select a key.

- **Edit XML Preferences**
  Select this option to edit the XML policy preferences. To edit the XML policy, click **Edit Preferences**.

**Warning:** Do not use the XML Preferences Editor without assistance from Symantec Support. If you misconfigure the preferences, Symantec Drive Encryption may not work properly.
Key Settings

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

Key Generation Settings

The settings on the Generation tab are:

- **Type**
  Select the default key type, RSA or DH/DSS, for your Symantec Drive Encryption users. The default setting is RSA.

- **Generate separate signing subkey**
  Select this option to permit your Symantec Drive Encryption users to generate separate signing subkeys.

- **Key Size**
  Select this option to set the default key size for your Symantec Drive Encryption users. The default setting is 2048.

- **Supported Ciphers**
  Deselect the ciphers that you do not want your Symantec Drive Encryption users to use.

- **Preferred Cipher**
  Select the supported cipher that you want your Symantec Drive Encryption users to use if no algorithm is specified. The default cipher is AES.

- **Supported Hashes**
  Deselect the hash types that you do not want your Symantec Drive Encryption users to use.

- **Preferred Hash**
  Select the supported hash that you want your Symantec Drive Encryption users to use if no hash is specified. The default hash is SHA-2-256.

- **Supported Compression**
  Deselect the compression types that you do not want your Symantec Drive Encryption users to use.
  
  If you select **None**, data is not compressed before it is encrypted.

- **Preferred Compression**
  Select the supported compression type that you want your Symantec Drive Encryption users to use if no compression type is specified. The default compression type is ZLIB.
Establishing Symantec Drive Encryption Client Settings

Key Settings

- **Auto-Renew Keys Every**
  Select an auto-renewal period for the keys of your Symantec Drive Encryption users. Internal keys are automatically renewed in the period you specify, unless they have exceeded the inactivity threshold that you selected in **Stop Renewing After**.
  
  If you do not want the internal keys to expire, despite inactivity, select **Never renew**.

- **Stop Renewing After**
  Select inactivity period for the keys of your Symantec Drive Encryption user. Internal keys are no longer renewed automatically after a period of inactivity.
  
  If you want your internal keys to renew continually, select **Never stop renewing**.
  
  If you set a short auto-renewal period, you enable the Symantec Encryption Management Server to manage itself and reduce the need to manually delete a user in the event someone leaves your organization. Consider how long a period of inactivity should be before you reasonably conclude that a user account is no longer in use.

Key Mode Settings

Use the options on the **Management** tab to select which key modes your Symantec Drive Encryption users can use when they create keys. You must select at least one key mode.

The decision that you make now selecting a key mode affects how you can deploy and use other Symantec Corporation products.

The settings on the **Management** tab are:

- **Server Key Mode (SKM)**
  Select this option to use the Symantec Encryption Management Server to generate and manage the keys of your Symantec Drive Encryption users.

- **Client Key Mode (CKM)**
  Select this option to permit your Symantec Drive Encryption users to generate and manage their own PGP keys.

- **Guarded Key Mode (GKM)**
  Select this option to permit your Symantec Drive Encryption users to generate and manage their own keys, and to store encrypted backup copies of your users' private keys on the Encryption Management Server.

- **Server Client Key Mode (SCKM)**
  Select this option to store the private encryption keys that are shared between your Symantec Drive Encryption users and the Symantec Encryption Management Server, and private signing keys only on the client systems.

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 this option to use the consumer’s username as the common name to which the certificate is issued.

- **Country (C)**
  Select this option to specify the country.

- **State/Province (ST)**
  Select this option to specify the name of the state or province.
  Do not abbreviate the state or province name. For example, type “California” not “CA”.

- **Locality (L)**
  Select this option to specify the name of the city or locality.

- **Organization (O)**
  Select this option to specify the name of your organization or company.

- **Organizational Unit (OU)**
  Select this option to specify the name of your organization’s unit.

- **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**
  Use this option to generate certificates to have the same usage flags that are on the matching PGP key.

- **Set non-repudiation key usage**
  Select this option to permit your Symantec Drive Encryption users with non-repudiation key usage to sign S/MIME messages with non-repudiation.
  Non-repudiation is a usage flag specific to X.509 certificates. Non-repudiation provides assurance of the source and integrity of the message and may be required in some environments.

**Allowed Key Usages** controls what usage flags (certificate attributes) a generated certificate has permissions to request. It does not control what usage flags the certificate actually has.

- **Digital Signature (digitalSignature)**
  Select this option if you want the certificate to have a signing usage flag.
Establishing Symantec Drive Encryption Client Settings

Key Settings

- **Non-repudiation (nonRepudiation)**
  Select this option if you want the certificate to contain a non-repudiation usage flag. This option does not actually apply the non-repudiation usage flag.
  
  If you want the certificate to be used for non-repudiation, you must select **Non-repudiation (nonRepudiation)** and **Set non-repudiation key usage**.

- **Key Encipherment (keyEncipherment)**
  Select this option to use the certificate to encrypt other keys or certificates.

- **Data Encipherment (dataEncipherment)**
  Select this option to use the certificate for encryption.

- **Key Agreement (keyAgreement)**
  Select this option to use the certificate for key exchange protocols. For example, Diffie-Hellman key exchange.

- **Encipher only (encipherOnly)**
  Select this option to use the certificate only for encryption.

- **Decipher only (decipherOnly)**
  Select this option to use the certificate only for decryption.

- **TLS WWW Server Authentication**
  Select this option to use the certificate for TLS/SSL server authentication.

- **TLS WWW Client Authentication**
  Select this option to use the certificate for TLS/SSL client authentication.

- **Email Protection**
  Select this option to use the certificate to use S/MIME to protect email messages.

- **Import X.509 certificates as drop-down list options:**
  - **PGP Bundle Keys**
    Select this option to bundle user X.509 signing and encryption certificates into a single identity.
    Symantec Corporation recommends this option.
  - **PGP Wrapper Keys**
    Select this option to import user X.509 signing and encryption certificates as separate identities.
    
    This option is not recommended because it only functions in an exclusively S/MIME environment.
  - **User selectable**
    Select this option to permit your Symantec Drive Encryption users to choose how to import their smartcard X.509 certificates.

- **Storage of keys on supported smart cards** drop-down list options:
  - **Attempt**
    Select this option to permit Symantec Drive Encryption to attempt to store new keys that your Symantec Drive Encryption users create on detected supported smartcards.
Establishing Symantec Drive Encryption Client Settings

Key Settings

Users are not required to have a supported smartcard to create a new key.

- **Require**
  
  Select this option to require new keys that your Symantec Drive Encryption users create to be stored on a supported smartcard. Users cannot create a key unless Symantec Drive Encryption detects a supported smartcard on which to store.

- **Disable**
  
  Select this option to disable the storage of keys on supported smartcards.

- **Use of CAPI-based credentials** drop-down list options:
  
  You can select Force, Prefer, or Ignore.

  If you want to use CAPI-based credentials, your Symantec Drive Encryption users’ private portion of their certificates must be in the CAPI store.

Options Settings

The settings on the Options tab are:

- **Allow users to receive encrypted email.**
  
  Select this option to permit your Symantec Drive Encryption users to receive encrypted email. Deselect this option to disable the feature and prevent your users from receiving encrypted email.

- **Enforce minimum passphrase length of X characters.**
  
  Select this option to require a minimum number of characters in passphrases for new keys that your Symantec Drive Encryption users create. The default number of characters is eight.

- **Enforce minimum passphrase quality of X%.**
  
  Select this option to require a minimum passphrase quality level for new keys that your Symantec Drive Encryption users create.

- **Saving passphrases**
  
  Select one of the following options to apply when your Symantec Drive Encryption users provide their passphrases:

  - **Save passphrases for the current session only**
    
    Select this option to automatically save passphrases in memory until your users log off their computers.

    Your users are prompted for their passphrase once per private key. They are not prompted to provide it again for the same key until they log off their computers.

  **Caution:** If you select this option, make sure that your users log off their computers before they leave them unattended. Passphrases can remain cached for weeks if they never log off, which allows anyone to read their encrypted messages or encrypt messages with their key while they are away from their computer.
Symantec Encryption Desktop Settings

You can use the following ways to control what your users can do with Symantec Drive Encryption clients after it is installed on their systems:

- **License settings**
  
  You can purchase licenses that contain only the features that you want to support. For example, if you want your users to encrypt their drives, then you purchase licenses that include Symantec Drive Encryption.

- **Feature settings**
  
  You can configure the settings for the features that your security policies support. For example, you purchase a license that includes Symantec Drive Encryption. You can control if removable USB disks inserted on your users’ systems must be encrypted.

- **Feature control**
  
  You can control which features are installed on your Symantec Drive Encryption clients. Features that you disable do not appear in the Symantec Drive Encryption console.

  Feature control is available only for the primary features of Symantec Drive Encryption.

  For example, you have licenses that support PGP Shredder, but you have a subset of users that do not require this feature, you can create a client installer just for this subset of users.

  This setting is available for Windows clients only.

- **Component control**
  
  You can control which components your Symantec Drive Encryption clients can use. You can edit the MSI client installer file and disable Symantec Encryption Desktop components. Components that are disabled do not appear in the Symantec Encryption Desktop console.

  For example, you do not use Lotus Notes or Groupwise for messaging. You can disable these components to limit any potential compatibility issues. You can use Microsoft’s msiexec application to disable components after you create the client installer file.

- **Save passphrases for X (hh:mm:ss)**
  
  Select this option to automatically save passphrases in memory for a specified period.

  Your users are prompted for their passphrases once for the initial signing or decrypting task. They are not prompted to provide it again until the specified time has elapsed. The default setting is 0:3:0 (3 minutes).

- **Do not save passphrases**
  
  Select this option to prevent your users’ passphrases from being stored in memory.

  Your users must provide their passphrase each time it is required.
To enable a component that you disable, you must reinstall Symantec Encryption Desktop with component enabled.

For more information, see *Controlling Symantec Drive Encryption Components* (on page 63).

The 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 – Best Practices**

As a best practice, Symantec recommends that you enable specific settings on the General tab. These recommendations improve your Symantec Drive Encryption users’ experience. They also help keep your clients current while lessening the load on your clients and the Encryption Management Server.

The recommended settings on the General tab are:

- **Enable Silent Enrollment.**
  Select this option to reduce the pages that your users must navigate during enrollment. When you reduce the number of pages, you reduce user input errors.

- **Download policy updates from Symantec Encryption Server every X hours.**
  Select this option to keep your clients current without overloading communications between your clients and the Encryption Management Server. Keep the default time setting of every 24 hours.

**General Tab – Settings**

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

The options on the General tab are:

- **Allow users to change options.**
  Select this option if you want to enable your Symantec Drive Encryption users to change the settings that you established.
  Deselect this option to prevent them from changing these settings.

- **Allow user-initiated key generation.**
  Select this option if you want to enable your Symantec Drive Encryption users to create new keys and subkeys, in addition to the key that was created during installation. This option also enables your users to make specific changes to their keypairs, such as adding and removing ADKs, appointing and removing third-party key revokers, or creating and using subkeys.
  Deselect this option to prevent them from creating new keys after installation and from making specific changes to their keypairs.

- **Allow user-initiated key signing.**
  Select this option if you want to enable your Symantec Drive Encryption users to sign keys.
Deselect this option to prevent them from signing keys and to enforce centralized control over the validity of keys.

- **Allow conventional encryption and self-decrypting archives.**
  Select this option if you want your Symantec Drive Encryption users to use a passphrase instead of a key to encrypt files conventionally, or to create self-decrypting archives (SDAs).
  **Caution:** Conventionally encrypted and self-decrypting files cannot be decrypted by your organization’s ADK, which may conflict with your data recovery policy.
  Deselect this option to prevent them from conventionally encrypting files or creating SDAs.

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

- **Automatically synchronize keys with servers.**
  Select this option if you want Symantec Drive Encryption to automatically keep your users’ keys synchronized with configured servers. 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.**
  Select this option if you want to set up automatic key reconstruction 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 *Reconstructing Keys with Symantec Encryption Server* in the *Symantec Encryption Desktop User's Guide*.

- **Override default keyring locations.**
  Select this option if you want to override the default locations for Windows and Mac OS X systems. Your Symantec Drive Encryption users' keyrings are created in and backed up to the locations that you specify instead of to the default keyring locations.
  - **Windows systems**
    The default keyring location is:
    \`C:\Documents and Settings\[user]\My Documents\PGP\`
  - **Mac OS X systems**
    The default keyring location for Mac OS X is:
    \`[user]/Documents/PGP/`
Establishing Symantec Drive Encryption Client Settings

Note: If you use this option, Symantec Encryption Desktop still requires temporary access to the My Documents folder on the Symantec Drive Encryption user’s system. If your IT policy restricts access to the My Documents folder, temporarily enable access to this folder during Symantec Encryption Desktop installation.

- **Enable Silent Enrollment.**
  Select this option if you want to reduce the pages that your Symantec Drive Encryption uses must navigate through during enrollment.
  Only essential Setup Assistant pages open during enrollment; non-essential pages are suppressed and the default settings are used.
  
  Note: To enable silent enrollment, you must use LDAP Directory Synchronization and then on the Drive Encryption tab, set the Allow/Deny/Require encryption of disks to existing Windows Single Sign-On password option to Require.

  See Drive Encryption Tab on page 50.

- **Activate FIPS 140-2 operational and integrity checks.**
  Select this option if you want to activate FIPS operational tests on your Symantec Drive Encryption users' systems the next time Symantec Drive Encryption starts. FIPS operational tests may slow performance on those systems.

- **Show Symantec Encryption Desktop in system tray/menu.**
  Select this option if you want the Symantec Encryption Desktop padlock icon to appear in the system tray of your Symantec Encryption Desktop users when Symantec Encryption Desktop is active on their systems.
  This option also lets your users access some of the Symantec Encryption Desktop features without launching the application first.
  Deselect this option if you want to hide the icon.

- **Hide the option to disable PGP Services.**
  Select this option if you do not want the Stop PGP Services option to appear on the PGP Tray menu for your Symantec Drive Encryption users. Hiding this option prevents your users from disabling Symantec Drive Encryption services on their system.

- **Send client logs to Symantec Encryption Server every X minutes.**
  Select this option if you want to specify how often Symantec Drive Encryption client logs are sent to the associated Symantec Encryption Management Server console. The default setting is 5 minutes.

- **Download policy updates from Symantec Encryption Server every X hours.**
  Select this option if you want to specify how often the Symantec Drive Encryption client downloads policy updates from the associated Symantec Encryption Management Server console. The default setting is 24 hours.
Establishing Symantec Drive Encryption Client Settings
Symantec Encryption Desktop Settings

Messaging & Keys Tab

The settings 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 settings on the Messaging & Keys tab are:

- **Email Messaging.**
  Deselect this option to disable the Email Messaging feature. This feature no longer appears in the Symantec Encryption Desktop console.

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

- **Enable encrypt and sign buttons in Outlook MAPI for Windows.**
  Select this option to permit your Symantec Drive Encryption users to encrypt and sign email. When you select this option, the encrypting and signing options appear in Microsoft Outlook.

- **Enable Out Of Mail Stream support (OOMS).**
  Select this option to permit your Symantec Drive Encryption users to send emails per policy in support of Web Email Protection or Smart Trailers when the Symantec Encryption Management Server is out of the mailstream.
  Deselect this option to prevent your Symantec Drive Encryption users from sending these messages if the Symantec Encryption Management Server is out of the mailstream.

- **Allow outbound PGP/MIME from Windows MAPI accounts.**
  Select this option to allow MAPI to use PGP/MIME to encrypt, and encrypt and sign messages.
  Deselect this option to allow MAPI to uses PGP Partitioned.
  MAPI can send messages PGP/MIME signed whether this setting is enabled or disabled.

- **Add a comment to secured email.**
  Select this option to append the text in the box to clear-signed PGP blocks, including exported key files, and encrypted files and text.
  Deselect this option and leave the box empty if you do not want append a comment to these messages.

- **Sign email stored in IMAP/MAPI sent message folders.**
  Select this option to permit your users Sign, Encrypt, and Encrypt and Sign messages stored in IMAP/MAPI sent message folders on their systems.
Establishing Symantec Drive Encryption Client Settings

Symantec Encryption Desktop Settings

- **Match IMAP folder name patterns.**
  Select this option to add additional IMAP folder name patterns that you want to secure. You can use a wildcard *. Not case sensitive.
  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 that you want to secure.

- **Allow users to follow local client policy.**
  Select this option to permit your Symantec Drive Encryption users to take actions that follow local client policy, but override the mail policy of the Symantec Encryption Management Server.
  This option lets your users create messaging policies that might make their messaging less secure.
  Deselect this option to prevent your users from overriding mail policy.

- **Mail policy.**
  Select this option to control what happens to email when Symantec Drive Encryption cannot reach the Symantec Encryption Management Server.
  - Standalone
  - Offline: Standalone
  - Offline: Block
  - Offline: Send Clear

- **If client fails to download policy for X days.**
  Select this option to establish how your Symantec Drive Encryption clients handle situations where policy cannot be downloaded from the Symantec Encryption Management Server console for the specified period.
  - Block outbound message.
    Select this option to block outbound messages when policy cannot be downloaded for the specified period.
  - Apply last downloaded policy.
    Select this option to use the last policy downloaded when policy cannot be downloaded for the specified period.

- **Use current PGP issued X.509 certificates instead of existing X.509 certificates.**
  Select this option 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 their certificate in Lotus Notes.
  The Lotus Notes certificate is suppressed.

- **Add PGP issued X.509 certificate to Lotus Notes if no X.509 certificate exists.**
  Select this option to insert the PGP certificates into the Lotus Notes certificate directory, whether the user has another certificate or not.
  This option is only available if you selected **Use PGP certificates instead of Lotus Notes certificate.**

- **Prefer Notes native encoding over PGP encoding.**
  Select this option if you are using Lotus Notes mail servers with Windows Notes clients and you want to use native Notes encoding.
Establishing Symantec Drive Encryption Client Settings
Symantec Encryption Desktop Settings

- **Instant Messaging.**
  Select this option to permit you users to use the Instant Messaging feature.
  Deselect this option to disable the Instant Messaging feature. The feature does not appear in the Symantec Encryption Desktop console.

- **Encrypt/Decrypt AOL Instant Messenger conversations.**
  Select this option to protect the AOL instant messages (IMs) between your Symantec Drive Encryption users and other Symantec Drive Encryption or Symantec Encryption Desktop users.

  **Caution:** Instant messages are protected only if both users are running Symantec Drive Encryption or Symantec Encryption Desktop software, and both users have this setting enabled.

  Deselect this option if you do not want to protect or do not use these instant messaging sessions.

- **Key Management.**
  Select this option to permit your users to manage their keys.
  Deselect this option to disable the Key Management feature and prevent your users from managing their keys. This feature does not appear in the Symantec Encryption Desktop console.

**Zip & Shredder Tab**

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

The settings on the **Zip & Shredder** tab are:

- **PGP Zip**
  Select this option to permit your users to put any combination of files and folders into a single encrypted, compressed package for convenient transport or backup.
  Deselect this option to disable the PGP Zip feature. The feature does not appear in the Symantec Encryption Desktop console.

- **PGP Shredder**
  Select this option to permit your users to completely destroy files and folders so that even file recovery software cannot recover them.
  Deselect this option to disable the PGP Shredder feature. The feature does not appear in the Symantec Encryption Desktop console.

- **Number of shredder passes**
  Type how many shredder passes your Symantec Drive Encryption users can use when they shred. The default setting is three passes.
  Note that more passes increase the security of the shred but more passes also increases how long the shredding process takes to complete.

- **Warn user before shredding files**
  Select this option to warn your Symantec Drive Encryption users before files on their system are shredded.
Deselect this option to suppress this warning.

- **Automatically shred when emptying the Recycle Bin/Trash**
  Select this option to shred the files that your users delete from their Recycle Bins or Trash.
  Deselect this option to prevent deleted files from being shredded.

### File Share Tab

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

The settings on the **File Share** tab are:

- **Symantec File Share Encryption for Windows**.
  Does not apply to Symantec Drive Encryption users.
  Deselect this option to disable the Symantec File Share Encryption feature. The feature does not appear in the Symantec Encryption Desktop console.

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

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

- **Force the encryption of files in the following folders**.
  This feature does not apply to Symantec Drive Encryption users.

- **Prevent the encryption of files in the following folders**.
  This feature does not apply to Symantec Drive Encryption users.

- **Force the encryption of files associated with the following applications**.
  This feature does not apply to Symantec Drive Encryption users.

- **Prevent the automatic decryption of files by the following applications**.
  This feature does not apply to Symantec Drive Encryption users.
Drive Encryption Tab – Best Practices

As a best practice, Symantec recommends that you enable specific settings on the Drive Encryption tab. These recommendations improve your users’ experience, help prevent hard drive corruption, and improve security.

The recommended settings on the Drive Encryption tab are:

- **Allow encryption of disks to existing Windows Single Sign-On password.**
  
  Select this option and then select Allow to permit your users to log in once for both Symantec Drive Encryption and Windows. Single sign-on improves the user experience and improves security. Domain passwords expire and must be changed periodically.

  **Note:** Verify that your users’ Windows accounts, passwords, and domains are up-to-date.

- **Automatically encrypt Boot disk at installation.**
  
  Select this option to ensure that the boot drive starts encryption as part of the enrollment process without user participation.

- **Force power failure safety.**
  
  Select this option to protect your hard drives from being corrupted during encryption if a power failure occurs. Initial encryption may take longer when you enable Power failure safety.

  To use this option, you must select **Automatically encrypt Boot disk at installation.**

- **Lock passphrase user accounts on Windows clients after 5 failed login attempts.**
  
  Select this option to prevent excessive authentication attempts.

  When you prevent excessive authentication attempts, you reduce the chances that unauthorized users have to gain access to a computer that is lost or stolen. When you set the failed log in number to five, you still provide your users a reasonable number of attempts to log in successfully.

- **Enable Whole Disk Recovery Tokens.**
  
  Select this option to provide your users with a means to access their computer if they forget their password or their account is locked.

- **Allow configuration of Drive Encryption Local Self Recovery for Windows clients.**
  
  Select this option to provide your users a means to recover from a disk lockout without contacting you. They only need to answer questions that they previously defined.

  **Note:** This setting also applies to Linux clients.
Establishing Symantec Drive Encryption Client Settings

Symantec Encryption Desktop Settings

- **Encrypt Windows Drive Encryption disks and PGP Virtual Disks to a Disk Administrator Key.**
  
  Select this option to provide a means to unlock an encrypted disk in abnormal situations. For example, a whole disk recovery token is not available; a user is not available; or legal reasons require it.

**Drive Encryption Tab – Settings**

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

*Note:* Some features of Symantec Drive Encryption 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, these features are ignored. All other settings work as configured.

The settings on the Drive Encryption tab are:

- **PGP Virtual Disk.**
  
  Select this option to permit your Symantec Drive Encryption users to use part of their hard drive as an encrypted virtual disk volume.

  Deselect this option to prevent your Symantec Drive Encryption users from using part of their hard drive as an encrypted virtual disk volume. Deselecting this option disables the feature, and removes the option from your users’ Symantec Drive Encryption console.

- **Automatically create PGP Virtual Disk on Windows clients upon installation.**
  
  Select this option to automatically create a PGP Virtual Disk volume for your Symantec Drive Encryption users to use. The virtual disk volume is created with the capacity and format that you specify.

- **Unmount when inactive for X minutes.**
  
  Select this option to automatically unmount the PGP Virtual Disk volumes of your Symantec Drive Encryption users after a specified time (in minutes) of system inactivity.

  This option helps prevent unauthorized persons from accessing the protected data on a PGP Virtual Disk volume. This functionality can be useful, for example, if a user leaves work and forgets to unmount a virtual disk volume.

  Deselect this option to prevent the PGP Virtual Disk volumes of your users from automatically unmounting because of system inactivity.

- **Unmount on system sleep.**
  
  Select this option to automatically unmount the PGP Virtual Disk volumes of your Symantec Drive Encryption users if their systems go to sleep.

  Before you select this option, make sure that your systems support sleep mode.

  Deselect this option to prevent PGP Virtual Disk volumes of your users from automatically unmounting if their system goes to sleep.

- **Prevent sleep if disk(s) cannot be unmounted.**
  
  Select this option to prevent your Symantec Drive Encryption users systems from going to sleep if a PGP Virtual Disk volume cannot unmount.
This option can help to prevent data loss that might occur if a PGP Virtual Disk volume is still mounted when a system goes to sleep.

Deselect this option to permit your users’ systems go to sleep even if the PGP Virtual Disk volume cannot unmount.

- **PGP Portable.**
  Deselect this option to prevent your Symantec Drive Encryption users from creating PGP Portable disks.
  Select this option to permit your users to create PGP Portable disks. PGP Portable requires a separate license.

- **Symantec Drive Encryption.**
  Select this option to permit your Symantec Drive Encryption users encrypt the contents of their system or specified USB flash drive.
  Deselect this option to prevent your users from encrypting the contents of their system or specified USB flash drive. Deselecting this option disables the feature, and removes the option from your users' Symantec Drive Encryption console.

- **User-Initiated Drive Encryption Permissions.**
  Use the following options to specify which encryption tasks your Symantec Drive Encryption users can do with internal and removable disks:
  - **Allow User Management.**
    This option permits your Symantec Drive Encryption users to add or remove other passphrase users from their internal and/or removable disks.
  - **Allow Encryption.**
    This option permits your Symantec Drive Encryption users to initiate encryption of internal and/or removable disks. This option does not affect automatic disk encryption during setup.
  - **Allow Decryption.**
    This option permits your Symantec Drive Encryption users to initiate decryption of internal and/or removable disks.
    If you deselect this option, users cannot decrypt disks. This option does not affect decryption after license expiration.

- **Store decryption policy on fixed disks.**
  Select this option to store the policy that specifies if your Symantec Drive Encryption users can initiate decryption of the disk on the encrypted disk. This information is not stored on removable disks.
  When you store the policy on the disk, you prevent current and future versions of Symantec Drive Encryption, Windows PE tools, and other recovery methods from decrypting the disk.

- **Allow/Deny/Force encryption of disks to existing Windows Single Sign-On password.**
  The Single Sign-On feature permits your Symantec Drive Encryption users to log into Symantec Drive Encryption and Windows at the same time. The SSO feature is only available for Windows clients.
After you select the Symantec Drive Encryption option, you can decide how to use the Single Sign-On (SSO) feature.

- **Allow**
  Select this option to permit your users to decide if they want to use the SSO feature.

- **Deny**
  Select this option to prevent your users from using the SSO feature.

- **Force**
  Select this option to require your users to use the SSO feature.

**Note:** You can leverage the Single Sign-On feature to enforce Symantec Drive Encryption passphrase quality alignment with your corporate passphrase quality requirements.

- **Automatically encrypt <volume type> at installation.**
  Select this option to encrypt the boot disk, only the boot partition, or only the Windows partition when Symantec Drive Encryption is installed.
  Deselect this option to disable this feature.

- **Require <authentication method>.**
  Select this option if you want to specify an authentication method to secure the encrypted drive. If you select this option, you must select a “required” authentication method.
  To specify an authentication method, you must first select the **Automatically encrypt Boot disk at installation** option.

  The available authentication methods are:

  - **standard passphrase authentication**
    Select this option to require your Symantec Drive Encryption users to use a standard passphrase authentication to encrypt the drive. This is the default setting.
    The use of this option is dependent on your selection (**Allow**, **Deny**, or **Force**) for the encryption of disks to existing Windows Single Sign-On password option. If you set this option to **Deny**, the disk is encrypted to a passphrase. If you set this option to **Force**, the disk is encrypted to a Single Sign-On user.

  - **supported smart cards for hardware security**
    Select this option to require your Symantec Drive Encryption users to use a supported smart card—for example, an Aladdin eToken—to encrypt the drive. The drive cannot be encrypted until your users provide a supported smart card.
    You must configure the smart card before users can use it to encrypt a drive. In addition, the system must already have the appropriate drivers installed.
    **Note:** Keys created on smart cards and tokens are not compatible with Symantec Drive Encryption’s key reconstruction feature.

  - **Trusted Platform Module (TPM)**
    Select this option to require your Symantec Drive Encryption users to use a system with TPM hardware to encrypt the drive. The drive cannot be encrypted unless TPM hardware is present.
- **Force maximum CPU Usage.**
  Select this option to use more CPU cycles to speed up the drive encryption process. Some systems may experience lag during maximum CPU usage.
  
  To force maximum CPU usage, you must first select the **Automatically encrypt Boot disk at installation** option.
  
  Deselect this option to prevent the encryption process from using any extra CPU cycles.

- **Force power failure safety.**
  Select this option to enable system data recovery and to restart encryption if a power failure occurs during encryption. This feature may cause initial encryption to take longer.
  
  To force power failure safety, you must first select the **Automatically encrypt Boot disk at installation** option.
  
  Deselect this option to prevent system data recovery and an encryption restart if a power failure occurs during encryption.

- **Lock passphrase user accounts on Windows clients after 3 failed login attempts.**
  Select this option to 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 cannot log in again without using a WDRT or other token. If one user logs in with a WDRT or other token, the disk unlocks, and all passphrase users can log in again. An administrator with a Symantec Drive Encryption administrator key can also unlock the account.
  
  Without a WDRT or other token or an administrator key, the disk is permanently locked.

- **Enable automatic encryption or locking of removable devices.**
  Select this option to prevent protected data from being copied onto an unprotected removable device.
  
  This feature is only available for Windows clients. For more information, see *Working with Removable Disks* in the *Symantec Encryption Desktop for Windows User’s Guide*.
  
  If this option is selected, when the Symantec Drive Encryption user inserts an unencrypted removable device the Automatic Encryption dialog box opens and displays a warning that the device is to be mounted read-only or that the device is to be encrypted after the specified period.
  
  The options for unprotected removable device interaction are:

  - **Lock device as read-only and provide users with the option to encrypt with Symantec Drive Encryption (Windows clients only).**
    Select this option to mount the unencrypted device as read-only. Users can read the data on the device, but cannot save anything to it.
    
    If users want to save data on the device, they can opt to encrypt it instead.

  - **Encrypt with Symantec Drive Encryption on Windows clients: After 30 seconds, After 1 minute, After 2 minutes, After 5 minutes, Immediately.**
    Select this option to automatically encrypt the removable device after a specified period.
A dialog box opens and counts down to removable device encryption. When the countdown to encryption times out, the removable device on the system is encrypted.

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 encrypts the portable device to another private key, if one is available. If there is no other private key, the user is prompted to create a passphrase user account to use to encrypt the removable device.

If a Whole Disk Recovery Token is required for encryption, and the user attaches an unencrypted removable device to the client computer and Symantec Drive Encryption cannot reach the Symantec Encryption Management Server, Symantec Drive Encryption cannot encrypt the removable device, and it is automatically unmounted. The user receives 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.
  Select this option so that you (administrator) can remotely regain access to a drive that has been encrypted. For example, the usual authentication method is unavailable because a user forgets a passphrase.
  Deselect this option to disable this feature.

- Allow configuration of Drive Encryption Local Self Recovery for Windows clients.
  Select this option to provide your Symantec Drive Encryption users a method to access encrypted drives from the PGP BootGuard login screen if they have forgotten their passphrases.
  Users can log in by answering security questions that they previously configured instead of contacting you 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.
  Select this option to have Symantec Drive Encryption display a list of all users on that computer who have configured Local Self Recovery.

- Encrypt using AES-256/AES-128.
  Select this option to use AES-256/AES-128 to encrypt. 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.
  Select this option to add a public key that can be used to create a token-based user on a drive that your Symantec Drive Encryption users encrypt. Selecting this option provides a way to access the data on an encrypted drive or to decrypt the encrypted drive if the user is unable or unwilling.
  To import the public key, click **Import** and do one of the following:

  - Navigate to the public key file
    Use **Browse** to navigate to the public key file that you want to import. Use Symantec Encryption Desktop to create this file, if it does not already exist.
Select the file, click **Open**, and then click **Import**.

- Paste the block of the public key
  
  Select **Import Public Key Block**.
  
  Paste the key block of the public key that you want to import, and then click **Import**.

To use the token-based user to access the encrypted drive, the private key must be on a supported token/smart card. Use Symantec Encryption Desktop either to create a keypair on or copy a keypair to a supported token/smart card.

For more information about PGP keys and tokens/smart cards, see *Storing Keys on Smart Cards and Tokens* in the *Symantec Encryption Desktop User’s Guide*.

- **Encrypt Drive Encryption disks to a Disk Administrator Passphrase.**
  
  Select this option so that you can add a passphrase that permits a Symantec Drive Encryption administrator to log in at the PGP BootGuard screen. For example, you may need to create an account on an encrypted disk for a new user.

  To create a passphrase, click **Create**.

  This feature does not require a hardware token. This feature does not support Single Sign-On.

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

- **Display detailed authentication fields.**
  
  Select this option if you want detailed authentication text boxes to appear on the PGP BootGuard screen of your Symantec Drive Encryption users.

  For more information, see the Symantec Encryption Management Server online help.

- **Add additional text to the Encryption BootGuard login screen.**
  
  Select this option so that you can add additional text to the PGP BootGuard login screen for your Symantec Drive Encryption users to see. You can use one line of text, up to 80 characters, including spaces.

  Deselect this option to disable this feature.

- **Customize screen backgrounds.**
  
  Select this option so that you can add custom background images to the PGP BootGuard screen for your Symantec Drive Encryption users to see. You can also opt for a plain gray background. You can add an image for both the splash and the login screen.

  Deselect this option to disable this feature.

  - To add a background image:
    
    Select **Upload background image files**.
    
    Click **Browse** next to **Splash Screen** or **Login Screen**, and then select an image for one or both.

  - To display a plain gray background:
    
    Select **Display plain gray background**.
You must use the following specifications to customize the background images:

- **XPM files only.**
  
  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.

- **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).**
  
  To verify that you are using 8-bit RGB use a text box editor to look at the XPM header:

  8-bit values appear as #285A83 (one hex triplet)
  
  16-bit values appear as #28285A5A8383 (two hex triplets)

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

- **Enable audio cues.**
  
  (For Windows clients only) Select this option to use audio clues for specific actions that occur during the PGP Bootguard authentication process. These audio clues can help vision-impaired users navigate the PGP BootGuard process.

  Deselect this option to disable this feature.

  Selecting this option enables the user's system to play audible tone combinations during the PGP BootGuard authentication process. Each tone combination starts with a middle sound and is followed by a higher tone, another middle tone, or a lower tone.

  The three combinations are:

  - **Ready for passphrase/pin entry**
    
    The middle-middle tone combination plays to indicate that users can provide their passphrase or pin.

  - **Successful authentication**
    
    The middle-high tone combination plays to indicate successful authentication. The system then continues to boot.

  - **Unsuccessful authentication**
    
    The middle-low tone combination plays to indicate unsuccessful authentication (failure).

    On the BootGuard authentication screen, the passphrase text box is cleared for another authentication attempt.

  You cannot customize the tone combinations; you only can decide to enable or disable them.

  **Note:** If you change this setting, the client must reboot to implement the change.
Licensing Settings

On the Client Licensing page (Consumers > Consumer Policy > [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**
  - Name of the authorized user.

- **Licensee Organization**
  - Name of the authorized company.

- **Licensee Email**
  - Email address used to contact someone about the license.

- **Options**
  - Symantec Encryption Desktop features included with this license.
  - **Licensee Count**
    - No longer available with new licenses.
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 .......................................................... 59
Creating an Installer with Preset Policy .................................................................... 60
Creating an Installer with No Policy Settings ........................................................... 61

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, and 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, and 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 check box is selected. If it is not selected, select it.

8. Select Preset Policy Group.
Creating the Symantec Drive Encryption Client Installer

Creating an Installer with No Policy Settings

You can also select to embed policy and license information into the installer to force the clients to be disconnected from the Symantec Encryption Management Server. In this case, there is no connection between Symantec Encryption Desktop on your users’ systems and the Symantec Encryption Management Server. The client will not receive any updated policy information from the Symantec Encryption Management Server, even if the policy is updated on the server side. Policy information normally downloaded during installation is instead embedded in the installer itself.

**Caution:** Use this option carefully, as most product features do not work in this mode.

9 In the **Symantec Encryption Server** field, enter the Symantec Encryption Management Server you want the application to interact with. The Symantec Encryption Management Server you are using to create the installer is listed by default.

10 In the **Mail Server Binding** field, enter the name of the mail server you want bound to the Symantec Encryption Management Server. You must enter this information unless your users read mail directly from this Symantec Encryption Management Server. Customized client installations will not work without mail server binding. You can use the * wildcard character to bind automatically to any mail server. Mail policy will be enforced for any mail server to which the client connects. You can use the wildcard as follows: *, *.example.com, and example.*.com. If you are creating a binding for an internal MAPI email client, you must use the WINS name of the Exchange Server. If you are creating a binding for an internal Lotus Notes email client, you must use the fully qualified domain name of the Domino server.

11 Click **Download**. The Symantec Drive Encryption client installer is created and downloaded to your system.

---

**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**, and then click **Download** Symantec Encryption Desktop 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** check box is deselected. If it is selected, deselect it.
Click **Download**. The Symantec Encryption Desktop installer is created and downloaded to your system.
To control what your users can do with Symantec Drive Encryption, you can disable specific Symantec Drive Encryption components. You must use software to distribute your client installers. You must be able to use the software to specify switches to the msiexec.exe command line utility.

Note: This feature is available for Windows clients only.

When you disable a Symantec Drive Encryption component it does not appear in the Symantec Drive Encryption console. Because the component is disabled, it does not have compatibility issues with the operating system or third-party products.

Upgrades, including automatic upgrades, honor the disabled Symantec Drive Encryption components and do not enable the disabled components unless you specifically edit the MSI file to enable the disabled component.

The table lists the Symantec Drive Encryption components that you can disable and the effects of disablement.

<table>
<thead>
<tr>
<th>Component</th>
<th>What Gets Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISABLESSONENROLL</td>
<td>Invisible silent enrollment.</td>
</tr>
<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>MAPI PLUGIN</td>
<td>The Encrypt and Sign features in Microsoft Outlook.</td>
</tr>
<tr>
<td>MEMLOCK</td>
<td>The memory locking feature that keeps sensitive data from leaving volatile memory.</td>
</tr>
<tr>
<td></td>
<td>Disabling memory lock is available so that you can disable all kernel-level items,</td>
</tr>
<tr>
<td></td>
<td>if desired. You should generally not disable it unless you have a specific reason</td>
</tr>
<tr>
<td></td>
<td>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>PGP SET HWORDER</td>
<td>The Symantec Encryption Desktop check to ensure that it is at the top of the</td>
</tr>
<tr>
<td></td>
<td>network provider list.</td>
</tr>
<tr>
<td>PGPSILEENT FORCE LDAP</td>
<td>The setting that enables the disk to be encrypted to a local Windows password but</td>
</tr>
<tr>
<td></td>
<td>lets enrollment use LDAP credentials that are different then the local Windows</td>
</tr>
<tr>
<td></td>
<td>credentials.</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>
</tbody>
</table>
Creating an Installer with No Policy Settings

<table>
<thead>
<tr>
<th>Component</th>
<th>What Gets Disabled</th>
</tr>
</thead>
<tbody>
<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 pgpdesktop.msi PGP_INSTALL_[component]=0
```

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

You can use a single command to disable multiple Symantec Encryption Desktop components. For example:

```bash
> msiexec /I pgpdesktop.msi PGP_INSTALL_MAPI=0
    PGP_INSTALL_NOTES=0 PGP_INSTALL_LSP=0
```

To enable a Symantec Encryption Desktop component that was disabled, you must reinstall Symantec Encryption Desktop with the disabled component specifically enabled. For example:

```bash
> msiexec /I pgpdesktop.msi PGP_INSTALL_MAPI=1
```
After you create your Symantec Drive Encryption client installer with the desired settings for your Symantec Drive Encryption users, Symantec Corporation strongly recommends that you do not immediately deploy it. Instead, test your client installer on as many representative machines as you can. You can save yourself a lot of time by finding and solving problems with the installer before your full deployment.

If any of these tests have unexpected results, 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.
How you deploy the Symantec Drive Encryption client installer to your users depends on your unique circumstances. Note that you cannot use the Symantec Encryption Management Server, which manages your Symantec Drive Encryption clients, to deploy the client installer.

Before you deploy the client installer, do the following:

- Decide upon a timeline.
  You can roll the software out in waves, but loss of momentum and focus can cause deployment and installment to drag out longer than desired.
- Verify that you are deploying the correct versions.
  Select between 32-bit packages and 64-bit packages.

Common installer deployment methods:

- Use an enterprise software distribution system, such as SMS or Tivoli
- Download from a Web/file server
- Distribute on a CD, DVD, or thumb drive

If you want to control Symantec Drive Encryption components during deployment, make sure that your deployment software can specify switches to the msiexec.exe command line utility. See Controlling Symantec Drive Encryption Components (on page 63).
Symantec Corporation recommends that you take the following actions to help support your Symantec Drive Encryption users:

- Provide your users with a written statement about how they should use Symantec Drive Encryption and for what it must be used.
  
  Include a summary of your official corporate security policies and instruction on how they can use Symantec Drive Encryption to conform to those policies.

- Provide your users with information about Symantec Drive Encryption.
  
  Include the following information:
  - What Symantec Drive Encryption does
  - How you expect them to use Symantec Drive Encryption
  - What Symantec Drive Encryption does to their system
  - What to do if they have problems with Symantec Drive Encryption

  For more information about the content you might provide to your users, see The User Experience (on page 71).


  Instruct them to read the Quick Start Guide before Symantec Drive Encryption is installed 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/).

- Provide your users with information about the other resources that are available to them, including the built-in online help.

- Provide your users with information about the steps they should take to make sure that their drives are in good condition before they encrypt them. For example, they should check the drive for error and defragment the drive.

  To check the drive for errors, Symantec Corporation recommends that you use a third-party scandisk utility such as SpinRite or Norton Disk Doctor.

  To defragment the drive, Symantec Corporation recommends that you use the built-in Windows utility or a third-party utility, such as PerfectDisk.

- Provide your users with help desk contact information, in case they experience problems.

- Warn your users not to click **CANCEL** during enrollment. Symantec Corporation strongly recommends that once enrollment begins, users do not cancel the process.

- Set up a system so that each user can report a successful installation.
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 affect your Symantec Drive Encryption users during setup:

- You can configure drive encryption to begin automatically or you can let your users start the process manually sometime after installation.
- Drive encryption is a background process.
  - Your users can continue to use their systems while the drive is encrypted.
- The drive encryption process can be paused.
  - A user can manually pause drive encryption.
  - Drive encryption pauses if the system shuts down, restarts, or enters standby mode.
  - On laptops, drive encryption pauses if the system moves from AC to battery power.
  - Note that you can only start drive encryption on a laptop if it is on AC power.
- On rare occasions, the drive encryption stops and displays the "Unable to instrument disk" error message.
  - Some of the reasons this error occurs are:
    - Not enough contiguous space is available on the drive
    - Disk errors are discovered on the drive
    - Windows has reserved some of the space needed to encrypt the drive
  - To solve these problems have the user check the drive for errors, defragment the drive, and then restart drive encryption.

## 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).