Symantec™ Encryption Management Server

Upgrade Guide

3.3

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

Version 3.3.0. Last updated: November 2012.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

Symantec Home Page (*http://www.symantec.com*)

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

1 About the Symantec Encryption Management Server Upgrade Guide

This Upgrade Guide describes how to upgrade previous versions of Symantec Encryption Management Server to version 3.3.0 and how to migrate a cluster to version 3.3.0.

This section provides a high-level overview of Symantec Encryption Management Server.

What is Symantec Encryption Management Server?

Symantec™ Encryption Management Server is a console that manages the applications that provide email, disk, and network file encryption. Symantec Encryption Management Server with Symantec Gateway Email provides secure messaging by transparently protecting your enterprise messages with little or no user interaction. The Symantec Encryption Management Server replaces PGP Keyserver with a built-in keyserver, and PGP Admin with Symantec Encryption Desktop configuration and deployment capabilities.

Symantec Encryption Management Server also does the following:

- Automatically creates and maintains a Self-Managing Security Architecture (SMSA) by monitoring authenticated users and their email traffic.
- Allows you to send protected messages to addresses that are not part of the SMSA.
- Automatically encrypts, decrypts, signs, and verifies messages.
- Provides strong security through policies you control.

Symantec Encryption Satellite, a client-side feature of Symantec Encryption Management Server, does the following:

- Extends security for email messages to the computer of the email user.
- Allows external users to become part of the SMSA.
- If allowed by an administrator, gives end users the option to create and manage their keys on their computers.

Symantec Encryption Desktop, a client product, is created and managed through Symantec Encryption Management Server policy and does the following:

- Creates PGP keypairs.
- Manages user keypairs.
- Stores the public keys of others.
- Encrypts user email and instant messaging (IM).
- Encrypts entire, or partial, hard drives.
- Enables secure file sharing with others over a network.

Who Should Read This Guide

This Upgrade Guide is for administrators who will be upgrading Symantec Encryption Management Server or migrating the data in your organization's Symantec Encryption Management Server environment.

Common Criteria Environments

To be Common Criteria compliant, see the best practices in *PGP Universal Server 2.9 Common Criteria Supplemental*. These best practices supersede recommendations made elsewhere in this and other documentation.

Using the Symantec Encryption Management Server with the Command Line

You can use the Symantec Encryption Management Server command line for read-only access to, for example, view settings, services, logs, processes, disk space, query the database, and so on.

Note: If you modify your configuration using the command line, and you do not follow these procedures, your Symantec Support agreement is void.

Changes to the Symantec Encryption Management Server using command line must be:

- Authorized in writing by Symantec Support.
- Implemented by Symantec's partner, reseller, or internal employee who is certified in Symantec Encryption Management Server Advanced Administration and Deployment Training.
- Summarized and documented in a text file in `/var/lib/ovid/customization` on the Symantec Encryption Management Server.

Changes made through the command line may not persist through reboots and may become incompatible in a future release. When troubleshooting new issues, Symantec Support can require you to revert custom configurations on the Symantec Encryption Management Server to a default state.

Symbols

Notes, Cautions, and Warnings are used in the following ways.

Note: Notes are extra, but important, information. A Note calls your attention to important aspects of the product. You can use the product better if you read the Notes.

Caution: Cautions indicate the possibility of loss of data or a minor security breach. A Caution tells you about a situation where problems can occur unless precautions are taken. Pay attention to Cautions.

Warning: Warnings indicate the possibility of significant data loss or a major security breach. A Warning means serious problems will occur unless you take the appropriate action. Please take Warnings very seriously.

Getting Assistance

For additional resources, see these sections.

Getting product information

The following documents and online help are companions to the *Symantec Encryption Management Server Administrator's Guide*. This guide occasionally refers to information that can be found in one or more of these sources:

- **Online help** is installed and is available in the Symantec Encryption Management Server product.
- **Symantec Encryption Management Server Installation Guide**—Describes how to install the Symantec Encryption Management Server.
- **Symantec Encryption Management Server Upgrade Guide**—Describes the process of upgrading your Symantec Encryption Management Server.
- **Symantec Encryption Management Server Mail Policy Diagram**—Provides a graphical representation of how email is processed through mail policy. You can access this document via the Symantec Encryption Management Server online help.

  You can also access all the documentation by clicking the online help icon in the upper-right corner of the Symantec Encryption Management Server screen.
- Symantec Encryption Satellite for Windows and Mac OS X includes online help.
- Symantec Encryption Management Server and Symantec Encryption Satellite release notes are also provided, which may have last-minute information not found in the product documentation.

Technical Support

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

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization

- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, Africa	semea@symantec.com
North America, Latin America	supportsolutions@symantec.com

2 About Upgrading Symantec Encryption Management Server

This chapter describes how to upgrade previous versions of the product to version 3.3.0 for single, non-clustered, server.

Warning: If you have a hardware token Ignition Key or a Hardware Security Module (HSM), you must contact Technical Support before you migrate to Symantec Encryption Management Server 3.3 or later. Migrating requires that you create a new setting on the upgraded version of Symantec Encryption Management Server before you restore the backup file from your previous system. This setting can only be added through SSH access with the help of Technical Support. If you migrate to version 3.3 or later without adding this preference, you will be locked out of the user interface after the upgrade. As a result, you cannot use your hardware token Ignition Key to unlock your Symantec Encryption Management Server. This can also occur if you upgrade from 3.0.0 to 3.1.0 using a PUP update. If you do a PUP update from 3.0.0, you must edit the settings in your 3.0.0 installation BEFORE the update. If you are running version 3.0.1, you do not need to change any settings.

Warning: If you plan to migrate a *cluster* from version 2.12 SP4 to Symantec Encryption Management Server version 3.3.0, before you migrate, run the latest version of the pgpSyncUsers utility on your 2.12 SP4 cluster to ensure that the user data is consistent. For more information, see *Migrating a Cluster* (on page 19).

To migrate your data from version 2.12 SP4 to Symantec Encryption Management Server version 3.3.0, you need disk space that is 10 times the size of the backup file. (The backup file will be significantly smaller than the original database.) For example, if your version 2.12 SP4 backup file is 1 GB, you should have 10 GB of disk space to allow for the migration and re-expansion of your data into the 3.3.0 database.

Upgrade Licenses

Although the licensing mechanism for the Symantec Encryption Management Server and the managed Symantec Encryption Desktop has changed, if you have a valid subscription license or Perpetual 2.x License, you do not need a new license to use Symantec Encryption Management Server 3.3.0.

If you had Symantec Encryption Desktop licenses configured through Consumer (User) Policies, these licenses are still valid, and the appropriate features are enabled after you upgrade. If you install a new version of Symantec Encryption Management Server version 3.3.0, you cannot add your old Symantec Encryption Desktop licenses through the Client Licensing page on the **Consumer Policies** tab. To use your old Symantec Encryption Desktop licenses, you must restore a backup that includes your previous licenses.

Backing Up the Data and Organization Key

Before you upgrade, back up the Organization Key and all the data from your Symantec Encryption Management Server. You must back up your data to an external location, because installing the software deletes all data stored on your Symantec Encryption Management Server. If you do not (or cannot) use FTP to back up your data to an external location, contact Technical Support.

To back up your data and organization key

1. Access the **Organization Key** page by doing one of the following:
   - For 3.0 or earlier, select **Organization > Organization Keys**.
   - For 3.0 or later, select **Keys > Organization Keys**.
2. Click **Organization Key**.
3. Click **Export**.
4. Select **Export Keypair** and type the passphrase.
5. Click **Export.**

   This saves the Organization Keypair to your desktop.
6. Back up the server data and configuration to an external server location
7. Select **System > Backups**.
8. Click **Backup Location**.
9. Select **Save backups to a remote location**.
10. Type the relevant details.
11. Click **Save**.

    You must save the data in a location other than the Symantec Encryption Management Server, because the data on the Symantec Encryption Management Server is erased during installation.
12. Click **Backup Now**.
13. Type a name for your backup.
14. Click **Backup**.

Overview of the Upgrade Process

You can upgrade your Symantec Encryption Management Server in the following ways:

- **Migration**, where you back up data to an external location, install the new software version from a CD/DVD, and restore your data. For more information about installing from a CD/DVD, see the *Symantec Encryption Management Server Installation Guide*.

- **PUP Update**, where you download and install a PGP Update Package (PUP) file from your Symantec Encryption Management Server's administrative interface. This method automatically preserves your data and system settings. For more information on performing a PUP update, see the *Symantec Encryption Management Server Administrator's Guide*. Not all upgrades are available as PUP update files.
- **Migration and PUP Update**, where you must use both methods. Some upgrades require a migration where you must back up your system, install the new version of the software, and restore your backup. For example, you must migrate before you use a PUP update when you upgrade from version 2.x to 3.2 or later. You must migrate to 3.0.2 SP2 or 3.12 SP2 first. Then install the PUP file; for example, install the 3.3.0 PUP file for Symantec Encryption Management Server 3.3.0.

After the software is installed and the Setup Assistant has started, depending on how you want to restore your data, there are several paths you can take through the setup.

Note: The licensing mechanism for the Symantec Encryption Management Server and the managed Symantec Encryption Desktop has changed as of Symantec Encryption Management Server version 3.3. However, these changes have minimal effects on the upgrade process, because your existing Symantec Encryption Management Server and Symantec Encryption Desktop licenses are still valid after you upgrade. If you perform a migration, your previous licenses are restored, and the features that were previously enabled are still enabled.

The following applies to Symantec Encryption Management Servers that are running as stand-alone systems or clusters:

- Before you upgrade to Symantec Encryption Management Server 3.3.0, you must back up your data and your organization key to an external location.
- You can upgrade to Symantec Encryption Management Server 3.3.0 from these versions:
  - PGP Universal Server 2.12 SP4

    To upgrade from 2.12 SP4, you must back up your data, do a fresh install of 3.0.2 SP2 or 3.1.2 SP2, and restore your backed up data. Then you can do a PUP update to update to version 3.3.0.

    If you are running a version older than 2.12 SP4, you must upgrade to version 2.12 SP4.
  - Version 3.x

    To upgrade from version 3.x, you can do a PUP update to update to version 3.3.0.

When you install the software, the data on your system is deleted. You need the backed up data file and the Organization Key to encrypt and decrypt the backup file. For more information on installing the software from a DVD, see the *Symantec Encryption Management Server Installation Guide*.

Caution: To upload and restore backups of 2GB or larger through the Symantec Encryption Management Server Web interface, you need to contact Technical Support.

Upgrading Your Symantec Encryption Management Server to Version 3.3.0

The following procedures apply to Symantec Encryption Management Servers running as standalone systems and clusters.

Note: Upgrading to 3.3.0 requires installing 1 PUP file: PGPUniversal3.3.0.pup.

To upgrade from version 2.12 SP4 to version 3.2.1:

1. Log in to your Symantec Encryption Management Server administrative interface.
2. Back up your data.
3. Upgrade to one of the following versions by performing a fresh install:
   - 3.0.2 SP2
   - 3.1.2 SP2
4. Restore your data.
5. Select **System > Updates**.
6. Upload and install the PGPUniversal3.3.0.pup file for Symantec Encryption Management Server 3.3.0. The Software Updates page displays this new version number.

After the upgrade, the system reboots, updating the kernel.

To upgrade from version 3.x to Symantec Encryption Management Server 3.3.0:

1. Log in to your Symantec Encryption Management Server administrative interface.
2. Select **System** > **Updates**.
3. Upload and install the PGPUniversal3.3.0.pup file for Symantec Encryption Management Server 3.3.0. The Software Updates page displays this new version number.

After the upgrade, the system reboots, updating the kernel.

Verifying Your Upgrade

After you upgrade to the latest version of Symantec Encryption Management Server, you can verify whether the upgrade was successful. The verification process listed below assumes you used one of the following methods to upgrade your Symantec Encryption Management Server.

- Migration
- PUP update

To verify your upgrade - Migration Process

1. After Symantec Encryption Management Server restarts, log in.
2. Select **System > Backups**

   The migrated database schema may differ from the default schema in the current release. At the end of the migration, a schema diff tool detects any schema discrepancies.

   If discrepancies are found, an error message is written to the backup log. The following links appear:

   - **Download migration log file**
   - **Download backup log file**

   The backup log contains pointers to the line numbers in the migration log, where migration errors are detected. A typical error message in the backup log will look like:

   error found at line xxx in <migration log>

   a. Click the appropriate link.

   b. Open or save the log file and review it.

   c. Repair the discrepancy error(s).

   d. Select the link **Run migration script** to rerun the schema checker. If an error has been resolved, its link no longer appears.

   e. If errors remain, call Technical Support to resolve the errors and stop them from appearing. The download links will continue to appear until you resolve your errors and have upgraded successfully.

To verify your upgrade - PUP Updating Process

1. After Symantec Encryption Management Server restarts, log in.
2. Select **System > Updates**

   The migrated database schema may differ from the default schema in the current release. At the end of the upgrade, a schema diff tool detects any schema discrepancies. If discrepancies are found, an error message is written to the update log. The following links appear:

   - **Download migration log file**
   - **Download update log file**

   The update log contains pointers to the line numbers in the migration log, where update errors are detected. A typical error message in the update log will look like:

   error found at line xxx in <migration log>

   a. Click the appropriate link.

   b. Open or save the log file and review it.

   c. Repair the discrepancy error(s).

d Select the link **Run migration script** to rerun the schema checker. If an error has been resolved, its link no longer appears.

e If errors remain, call Technical Support to resolve the errors and stop them from appearing. The download links will continue to appear until you resolve your errors and have upgraded successfully.

Note: During PUP updates and migrations, for any release prior to version 3.2.0, ensure that the status of the **Allow users to receive encrypted email** check box is set in the **Consumer Policy** section as per your environment. For more information on the Consumer Policy, see the *Symantec Encryption Management Server Administrator's Guide.*

Schema Comparison Report

During the migration process a schema comparison report is generated showing errors that may have occurred during migration. After the migration process is complete, the administrator can download a zip file containing the migration log and the schema report.

- `/var/log/ovid/last_update_migration_error`
- `/var/lib/ovid/pgprep/schema_report.txt`

When an error occurs during migration an error bubble is displayed above the list section. The error bubble contains a message describing where in the migration process the failure occurred, and a link to download the zip file. There is also a link to run the migration script again in the error bubble notification.

Note: If there are no errors found during the migration process the error message and symbolic links do not appear.

To download migration log and schema report:

1. Complete the upgrade or migration process.
2. After the Symantec Encryption Management Server has rebooted, log in again to the administrative interface.
3. Select **Reporting> Logs**
4. From the **Log** list, select the type of log you want to download.
5. Select **Export...** button at the bottom of the screen.
6. Select the log file or schema report you wish to download.

Running Schema Comparison Tool in Standalone Mode

If the administrator has ssh privileges, the schema comparison tool can be used in standalone mode. In the standalone mode the administrator can generate a schema comparison report without going through the user interface.

To execute the comparison report:

- Enter `sh /usr/share/ovid/pgprep/compare-schema.sh> report.txt`

Best Practices for Upgrade

The information in this list helps you ensure that your upgrade is successful:

- Install and test the upgrade in a lab or staging environment before you integrate the upgrade into your network.
- Back up the Organization Key and all the data from your Symantec Encryption Management Server before you upgrade.

  You must back up your data to an external location, because the upgrade process deletes the data stored on your Symantec Encryption Management Server. If you do not (or cannot) use FTP to back up your data to an external location, contact Technical Support.
- Save a copy of the installation media, in case you need to revert to the previous version.
- During upgrade, the Symantec Encryption Management Server does not process email.

  Before you upgrade Symantec Encryption Management Server, you must temporarily remove it from the mailflow.

Reconfiguring the MTA

If your network includes an MTA, you should reconfigure it to prevent email routing through the Symantec Encryption Management Server.

To reconfigure the MTA

1. Do one of the following:
   - If your company's email route through your Symantec Encryption Management Server, configure your MTA to halt outbound email processing.
   - If email that matches the criteria in your MTA content filter routes through the Symantec Encryption Management Server, configure the MTA to queue this email.
2. Configure the MTA to queue incoming email that passes through the Symantec Encryption Management Server, such as signed and/or encrypted email.
3. Review the Symantec Encryption Management Server log files to ensure that email is not passing through the Symantec Encryption Management Server.
4. Upgrade your Symantec Encryption Management Server and restore your user data.
5. Reconfigure your MTA to resume routing email to the Symantec Encryption Management Server.

Note: You can find more information about moving to Symantec Encryption Management Server 3.3.0 on the *Symantec website* (*http://www.symantec.com*).

Supported Client and Symantec Encryption Management Server Version Combinations

Symantec Corporation supports backward compatibility for clients only. Symantec Encryption Management Server 3.3.0 supports managing policy of these versions and subsequent maintenance releases for each of the following:

PGP Desktop

- 10.0.0
- 10.0.1
- 10.0.2
- 10.1.0
- 10.2.0
- 10.2.1

Symantec Encryption Desktop

- 10.3.0

Note: Limited backward compatibility support means that legacy features, such as enrollment, policy download, logging and reporting are supported, but legacy clients cannot access the latest client features in Consumer Policy.

We recommend that you upgrade your Symantec Encryption Management Server and your clients, so that they are eventually on the same release. For the most current information on which client versions are supported, see the Knowledge Base.

Symantec Encryption Management Server 3.3.0 supports managing policy of these versions and subsequent maintenance releases for each of the following:

PGP Universal Satellite

- 3.0
- 3.0.1
- 3.1.0
- 3.2.0
- 3.2.1

Symantec Encryption Satellite

- 3.3.0

Note: Policy options for features that do not exist in supported legacy versions are ignored by those installations.

Configuring the Symantec Encryption Management Server After Migration

During configuration, the Setup Assistant transfers the saved data from the previous version into Symantec Encryption Management Server 3.3.0.

To upgrade and restore your data and configuration information:

1. Install the upgrade software as described in the *Symantec Encryption Management Server Installation Guide*.
2. In the Setup Assistant, begin the configuration.

   You can perform a **New Installation** or restore your back-up configuration and data in this process. If you perform a new installation, you can restore your backup later through the Symantec Encryption Management Server administrative interface.

   - For more information on using the Setup Assistant to configure the Symantec Encryption Management Server as a new installation, see the *Symantec Encryption Management Server Installation Guide*.
   - For more information on restoring your backed up configuration and data using the Setup Assistant, see *Restoring Configuration and Data* (on page 15).

Restoring Configuration and Data

Note: During migration the previous Symantec Encryption Management Server default data is restored to the values of the new release. The default data include key servers, dictionaries, mail policies, message templates, and consumer policies.

To restore backed up data after installing the server:

1. Access the Setup Assistant in the new server.
2. Proceed through the wizard and click **Forward**.
3. Read the End User License Agreement and click **I Agree** and **Forward**.
4. In the **Setup Type page**, select **Restore** and click **Forward**.
5. In the **Import Organization Key** page, upload a file with your Organization Key and click **Forward**.
6. In the **Upload Current Backup File** page, click **Choose File**, select the backup file that you want to restore, and click **OK**.
7. In **Upload Current Backup File** page, click **Forward**.

   To upload backups of 2GB or larger, contact Technical Support.

After the backup has installed, the Network Configuration Changed page appears and the server restarts automatically. You can also check the update or migration logs for the *Database migration check completed.* message. You are redirected to the Symantec Encryption Management Server administrative interface, and the server is configured with the settings from the backup file you selected.

Your Symantec Encryption Desktop license(s) have been restored with the appropriate Consumer Policy setting. If your existing Symantec Encryption Desktop licenses are valid, you do not have to use the new default Symantec Encryption Desktop client license. Your mail policy and proxy settings have been reproduced in the new mail policy feature. For more information on mail policy and reproducing your previous settings, see *Migrate Groups from Version 2.12 SP4* (on page 17), and the *Symantec Encryption Management Server Administrator's Guide*.

8 Proceed through the Setup Assistant until you have finished.

Symantec Encryption Management Server runs in the Learn Mode.

For more information on configuring the Symantec Encryption Management Server after the Setup Assistant is complete, see the *Symantec Encryption Management Server Administrator's Guide*.

Updating Your Symantec Encryption Web Email Protection Complete Customizations

As a result of some new Symantec Encryption Web Email Protection features, such as PDF Email Protection Secure Reply and the ability to provide X.509 certificates to external users, after you upgrade to Symantec Encryption Management Server 3.3.0, you must also update your Symantec Encryption Web Email Protection Complete Customizations. For more information on customizing Web Email Protection, see *Customizing Symantec Encryption Web Email Protection* in the *Symantec Encryption Management Server Administration Guide*.

To update your Symantec Encryption Web Email Protection Complete Customization:

1 Select **Services > Web Email Protection**.

2 In the **Customization** panel, click **Add Template**.

3 Read the Customization Notice and click **Continue**.

4 Select **Complete Customization** and click **Next**.

5 Click **Download** next to one of the displayed options.

6 Select a location to save the file and click **Next**.

You should save the downloaded files in the same location as the older customization files. This way, the appropriate files are updated.

7 Zip the locally updated files.

8 Type a template name and click **Next**.

The other fields are optional.

9 Click **Browse** to locate the local Zip file and click **Next**.

The uploaded customization template appears on the Web Email Protection page.

Migrate Groups from Version 2.12 SP4

Caution: After migrating from a previous version, you must ensure that the groups are in the correct priority order. If groups are incorrectly prioritized, users will not receive the correct policy settings.

In version 2.12 SP4, if a user can be matched to more than one user policy, the user received the policy with the name that was first in alphabetical order. Administrators could not change this ordering. In Symantec Encryption Management Server 3.3.0, because users can belong to more than one group, you must make sure that the policies are ranked correctly.

Migrating Mail Policy Settings from Version 2.0.x

If you upgrade from version 2.0.x, your proxy and external domain policy settings are automatically replicated in the new mail policy. This section explains the changes in mail policy in Symantec Encryption Management Server.

The new mail policy provides many more ways of processing email than the previous version. In the previous version, you created a policy for each external domain. Now mail policy applies to all email traffic to and from all domains, although you can apply special handling to messages to or from certain domains or subdomains.

There is no longer an implicit managed domain policy. Now, all mail policy is clearly and explicitly described and controlled.

You can apply mail policy to email based on many criteria through the creation of rules. Previously, you could only apply policy based on domain name. Now you can match on header, subject, sensitivity, or sender email ID, as well as many other options.

You can process email in many ways. The old external domain policy only permitted you to specify that email be encrypted and signed or sent clear. Now you can specify that email should be bounced or dropped, for example.

How Upgrading and Updating Affect Mail Policy Settings

When you upgrade to the latest version of Symantec Encryption Management Server, different things happen to mail policy depends on the upgrade method you choose.

- **Update:** If you update using a .pup update package, your current mail policy chains do not change. Any new chains or rules are not applied. If you later use the mail policy **Restore To Factory Defaults** feature, the newer version of the mail policy chains is installed.
- **Fresh Installation:** If you upgrade to the latest version by backing up your existing data, doing a fresh installation on a new computer, and then restoring the backed up data to the new installation, the old mail policy overwrites the new version. If you want to use the new mail policy rules, you must recreate them manually. See the Mail Policy Diagram to understand what the default rules are and which conditions and actions to use to recreate them.

3 Migrating a Cluster

This chapter describes how to upgrade a Symantec Encryption Management Server cluster to version 3.3.0.

For an overview of clustering in Symantec Encryption Management Server version 3.3.0, see *Clustering your Symantec Encryption Management Servers* in the *Symantec Encryption Management Server Administrator's Guide*.

Following are the paths to upgrade clusters, depending on what version of Symantec Encryption Management Server you are starting from:

- From version 3.x, install the PUP file on each cluster member by following the instructions given in the *Upgrading Your Symantec Encryption Management Server to Version 3.3.0* (on page 10) section. You do not need to remove the member from the cluster before upgrading.
- From version 2.12 SP4, follow the upgrade instructions given in this chapter, starting with the *Cluster Migration Overview* (on page 19) section.

Cluster Migration Overview

All cluster members have the same database and configuration information, so changes on one are replicated to the others. The cluster migration process preserves this relationship.

Your Primary server must be migrated first. As part of the backup restoration process, the Primary server's 2.12 SP4 data is migrated into the version 3.3 database. This server now acts as the sponsoring server for the other cluster members. As it is joined to the new 3.3.0 cluster, its data is replicated to each cluster member. The join process also attempts a limited automatic reconciliation of data that exists on the joining server. If Web Email Protection is running in the Home Server mode, the Web Email Protection data is migrated individually on the each cluster member and is not replicated to other cluster members.

If there are data inconsistencies or conflicts between the version 2.12 SP4 Primary and its secondary servers, the migration process may not be able to reconcile the inconsistencies. You can run the pgpSyncUsers utility that identifies data inconsistencies between your primary and secondary cluster members. If you customized your Symantec Encryption Management Server configuration you may have to perform the customizations again after you migrate your cluster. Contact Technical Support for more information.

Important: Before you install new software on any of your cluster members, run the pgpSyncUsers utility on your version 2.12 SP4 primary cluster member to ensure there are no data inconsistencies between your primary and secondary servers. Inconsistencies may cause user data to be migrated incorrectly. For instructions to access and use pgpSyncUsers, see the Knowledge Base.

Cluster Migration Requirements

All members of a Symantec Encryption Management Server cluster must run the same software version. Since member servers do not share the software upgrade, you must migrate each server individually. To upgrade a cluster successfully, you must run version 2.12 SP4 or later. If you are running an earlier version, you must upgrade to version 2.12 SP4 on each server.

The upgraded and restored Primary server acts as the sponsor for the other servers that join the cluster. You should upgrade all cluster members at the same time. If all the servers are down at the same time, email will not move through your network. For more information about temporarily stopping the mailflow, see *Best Practices for Upgrade* (on page 13).

Migrating Your Cluster

This process provides an overview of the cluster upgrade process.

1 Verify that your cluster members are running version 2.12 SP4 or later.

If your cluster members are running an earlier version, you must first upgrade to version 2.12 SP4.

2 Download, install, and run pgpSyncUsers to identify whether there is inconsistent data between your primary and secondary cluster members.

Inconsistent data may not migrate correctly to version 3.3.0. For more information, see *Cluster Synchronization Issues Before You Migrate* (on page 21). If your primary cluster member is already 3.x, you do not need to run the pgpSyncUsers utility.

3 Back up all cluster members to an external location.

From version 2.12 SP4, you must migrate (back up and restore) to one of the following and then PUP update to Symantec Encryption Management Server 3.3.0:

- PGP Universal Server 3.0.2 SP2
- PGP Universal Server 3.1.2 SP2

For more information on backing up your Symantec Encryption Management Servers, including their Organization Keys, see *Backing Up the Data and Organization Key* (on page 8).

4 Install Symantec Encryption Management Server 3.3.0 on your Primary server.

See *Upgrading Your Symantec Encryption Management Server to Version 3.3.0* (on page 10) for more information on your Symantec Encryption Management Server version and to restore its backup. This server is the sponsoring server that is used to recreate the cluster. After the restore, select **System** > **Clustering** in the Primary server's administrative interface to see the previous secondaries that are listed as pending cluster members.

5 Install Symantec Encryption Management Server 3.3.0 on each secondary server.

6 Restore each secondary's backup (from Step 3) before you join the secondaries to the new cluster.

Important: Do not use the **Cluster Member** option in the Setup Assistant.

You should back up the secondary sever if the original cluster was in home server mode. In high availability mode, only the Primary needs to be backed up because all cluster members share the same user data. It is always faster to update the Primary server and then join the secondary servers.

Note: If you see data inconsistencies, you must contact Technical Support.

7 After restoring the backup, on the previous secondary server, select **System > Clustering** and click **Join Cluster**.

8 Type the IP address of the previous Primary server, which is now the sponsoring server.

9 After the secondary server has requested to join a cluster, and is in a waiting state, select **System > Clustering**.

10 In the list of pending cluster members, click **Contact** next to the secondary server's name.

This step initiates the join and the data replication process. For more information on migrating your primary and secondary cluster members, see *Migrating your Primary Cluster Server* (on page 22) and *Migrating a Secondary Cluster Member* (on page 24).

When the cluster migration is complete, all cluster members have the replicated database and many of the same configuration settings. In a cluster from version 3.0 and later, all cluster members act as peers, where every server in the cluster serves all requests, and any server can initiate persistent changes.

Note: When you restore your data from a release earlier than version 3.0, some of the rules in the Outbound mail policy are lost. You must retype these rules manually.

Since Mail Policies are global, you can retype the rules on the sponsoring server before you join the other cluster members or on a cluster member after it has joined the cluster.

Cluster Synchronization Issues Before You Migrate

Before migrating a cluster to version 3.3.0, you must run the pgpSyncUsers utility on the Primary server in your 2.12 SP4 cluster to determine if there are data inconsistencies between your Primary and secondary servers. If the utility identifies data consistency or other data problems, contact Technical Support before you migrate your cluster. The migration process may not be able to reconcile data inconsistencies, and in some cases, inconsistent data from a secondary may be lost.

Remember the following:

- For more information on pgpSyncUsers, see the Knowledge Base.
- Your server 2.x cluster must be running version 2.12 SP4. If you are running a version earlier than 2.12 SP4, do a backup and restore to 3.0.2 SP2 or 3.1.2 SP2 and then a PUP update to version 3.3.0.
- To install and run the utility, you must have command line access via SSH to your Symantec Encryption Management Server cluster primary server. See *Accessing the Symantec Encryption Management Server using SSH* (on page 22) for more information.

Note: If the utility identifies inconsistencies in user data, contact Technical Support.

Accessing the Symantec Encryption Management Server using SSH

To access Symantec Encryption Management Server through the command line, you must create an SSHv2 key and add it to the superuser administrator account in Symantec Encryption Management Server. You can do this, for example, by using PuTTYgen to create an SSHv2 key and PuTTY to log in to the command line interface. You add the SSHv2 key to your superuser administrator account through the Symantec Encryption Management Server administrative interface.

PuTTY is a free suite of SSH tools that includes the following:

- PuTTYgen
- PuTTY
- PSFTP
- Pageant, the PuTTY authentication agent

The PuTTYgen and PuTTY.exe files can be downloaded separately from the Internet. To set up command line access to the Symantec Encryption Management Server, see the Knowledge Base.

Migrating your Primary Cluster Server

Before you migrate, you must ensure that your cluster members are running version 2.12 SP4 or later. If your cluster member is running an earlier version, you must upgrade to version 2.12 SP4.

To migrate your primary cluster

1. Download, install, and run pgpSyncUsers.

   Inconsistent data may not migrate correctly to version 3.3.0. For more information, see the Knowledge Base.

2. Back up your Primary Symantec Encryption Management Server, including the Organization Key, to an external location.

   For detailed information see *Backing Up the Data and Organization Key* (on page 8).

3. Follow *Upgrading Your Symantec Encryption Management Server to Version 3.3.0* (on page 10) to migrate your primary server to Symantec Encryption Management Server version 3.3.0.

   For more information on installing 3.3.0 and running the Setup Assistant, see the *Symantec Encryption Management Server Installation Guide*. In the Setup Assistant, you can select **New Installation** or **Restore**.

   Warning: Do not select **Cluster Member** for your Primary server.

4. If you selected **New Installation** in the Setup Assistant, in the administrative interface, select **System > Backups** to restore the backup to the former primary server.

5 After the restore is complete, select **System > Clustering** in the former Primary server to see the secondary servers appear as pending cluster members.

Until the secondary servers rejoin the cluster, their status remains as pending. The join action must be requested by each former secondary. The **Contact** button that appears next to each pending member does not have an effect until the former secondary server has migrated and requests a join to the cluster.

Note: For the sponsoring server to successfully contact the joining server, the hostname and IP address of the joining server must be resolvable via DNS. If not, the sponsoring server cannot contact the joiner, and the join will not succeed. If your cluster members do not have DNS resolvable hostnames, contact Technical Support.

---

6 After the secondary has been migrated to version 3.3.0 and has requested a join, in the sponsoring server's administrative interface, select **System** > **Clustering**.

7 Click **Contact** next to the secondary that is joining the cluster.

The joining cluster member's status changes from **Pending** to **Replicating**. This step initiates the join process, which involves replicating data from the sponsor to the new cluster member. The configuration settings for the Symantec Encryption Management Server you are installing as a cluster member, including administrator login and password, primary domain, and ignition key (if any) are replicated from the sponsoring server.

The join process also performs reconciliation of data that may have existed uniquely on the former secondary. For example, if your cluster was previously running Symantec Encryption Web Email Protection in Home Server mode, the join process migrates all Web Email Protection data that was kept on the secondary. If the database on the sponsoring server in a cluster has a large database, the join of a cluster member can take a long time. To avoid a join failure, you can increase the join timeout value setting before you start the join. This setting can only be modified through SSH access, with the help of Technical Support.

Symantec Encryption Management Server 3.3.0 allows you to specify whether a cluster member is located in your DMZ and whether it should be allowed to host private keys for internal users.

When you migrate a secondary from an earlier release, it is migrated with these default settings:

- Not located in the DMZ.
- Allowed to host private keys.

You can change these settings by selecting **System > Clustering > Edit Member** and clicking the cluster member name.

Note: Customers with databases larger than 1GB should use the manual join scripts instead of joining through the administrative interface.

After your cluster member has joined the cluster, you must restore your Outbound Mail Policy on one of the servers in your cluster by following the instructions in Restoring Mail Policy Rules. These changes are replicated to the other cluster members.

Migrating a Secondary Cluster Member

Before you perform the backups, run pgpSyncUsers to identify and correct data synchronization problems in your version 2.12 SP4 clusters.

To migrate a secondary cluster member

This procedure provides instructions to migrate your secondary cluster members.

1 Back up each of your secondary servers, including their Organization Keys, to an external location.

For more information, see *Backing Up the Data and Organization Key* (on page 8).

2 Follow the instructions in *Upgrading Your Symantec Encryption Management Server to Version 3.3.0* (on page 10) to migrate your secondary server to Symantec Encryption Management Server version 3.3.0.

Detailed instructions on installing the 3.3.0 software and running the Setup Assistant are found in the *Symantec Encryption Management Server Installation Guide*.

3 Restore the backup.

You should only back up the secondary servers when your cluster is running Web Email Protection in the home server (HS) mode. Otherwise, it is always more efficient to install Symantec Encryption Management Server 3.3.0 on the secondary servers and join these servers to the sponsor server. Typically, the following local server settings are not replicated:

- Network settings
- SMTP settings
- SNMP settings
- SSL/TLS certificates
- Backup
- Mail routes
- Mail proxies
- Mail queue
- Service access control
- Key cache

Your log files are not preserved during the migration. When you restore the backup, these settings and files are restored.

You may have to restore the backup to a secondary server under these conditions:

- You are not running Symantec Encryption Web Email Protection in HS mode or Web Email Protection was not running on this server.
- You do not need to preserve server-specific settings for mail routes, mail proxies, or external LDAP servers.
- You do not need to restore the SSL/TSL certificate for this secondary server.

For more information, see *Manually Reconfiguring Non-replicated Server Settings* (on page 25).

Note: Restoring the secondary nodes followed by a join will take more time.

4 After the restore, log in to the administrative interface of the former secondary server.

5 Select **System > Clustering** and click **Join Cluster**.

6 (Optional) Enter the hostname or IP address of the sponsoring server (the former primary server) and click **Save**.

After a warning, the joining server is put into a pending state until contact is initiated from the sponsoring server.

7 In the sponsoring server's administrative interface, select **System > Clustering** and click **Contact** next to the secondary that is in the **Wait** state.

8 The sponsoring server initiates the join and data replication.

9 Monitor the progress bar to track the replication.

Repeat these steps to migrate and rejoin all your former secondary servers to the version 3.3.0 cluster. We recommend that you always use the former primary server as the sponsoring server.

Manually Reconfiguring Non-Replicated Server Settings

If you do not plan to restore the backup onto a secondary server, but would like to preserve some non-replicated settings, you can individually restore those settings after you migrate to 3.3.0.

Important: You must back up the data from every cluster member to an external location. If you do not have individual settings for your secondary cluster members, rather than restoring the secondary backups, you can rely on the data replicated from your primary server.

To save specific, non-replicated settings

You must export or note the following, as appropriate to your installation.

1 Export your server SSL/TLS certificates.

a On each secondary server, select **System > Network** and click **Certificates** at the bottom of the dialog box.

b Select a certificate.

c Click **Export**.

The certificate is exported as a PKCS#12 file.

d Repeat this process for all the certificates you want to export.

2 Note the settings of your mail routes and proxies.

You need to re-configure these settings on the secondary after you install 3.3.0.

3 Select **Reporting > Logs**.

4 From the **Log** list, select **Mail**.

5 Click the Export button at the bottom of the screen, and select **Mail Log**.

The logs are saved in a separate location from the full backup.

To restore specific, non-replicated settings

After you install and configure the Symantec Encryption Management Server 3.3.0 on your former secondary server, and **before** you join this server to the new 3.3.0 cluster, you must restore your certificates, mail route, and mail proxy configurations. If you cannot manually restore your log files, and you want to restore the log files to a secondary server, you must restore the full backup.

1 If your secondary server used a different SSL/TLS certificate from the former primary server, import the certificate you exported in step c above.

   a When the replication is complete, log in to the cluster member's administrative interface.

   b Select **System > Network** and click **Certificates**.

   c Click **Add Certificates**.

   d Click **Import**

   You can import your saved PKCS#12 file in the **Import SSL/TLS Certificate** page.

2 In the cluster member's administrative interface, configure the appropriate mail routes and mail proxies.

   - Select **Mail > Mail Routes** and click **Add Mail Route**.

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

   - Select **Mail > Proxies** and click **Add Proxy**.

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

Changing Your Web Email Protection Message Replication Settings

In Symantec Encryption Management Server version 3.3.0, if you run Symantec Encryption Web Email Protection in a cluster, you can control how Web Email Protection message replication is handled.

You can still have Web Email Protection messages:

- Replicated to all cluster members (as in the former HA mode)
- Not replicated (as in the former HS mode).

You can now choose to have Web Email Protection messages replicated only to a subset of servers that are running Web Email Protection. This allows you to take advantage of the Symantec Encryption Management Server replication services without incurring the costs of replicating to all Web Email Protection servers in the cluster. For example, if you have four servers running Web Email Protection, you can Have messages replicated only to two of the four servers.

When the cluster migration from a version 2.12 SP4 cluster is complete, if this cluster was running in Home Server mode, Web Email Protection message replication is set to **Off**. If the cluster was running in HA mode, message replication is set to **All**. To change the message replication settings, select **Services > Web Email Protection**, and on the **Options** tab, click **Edit**. Since the message replication setting is global, you can Take this setting from the administrative interface of any cluster member.

Index