# Symantec Encryption Management Server Upgrade Guide 10.5

Last updated: July 2020

## Copyright statement

# Contents

# 1 About the Symantec Encryption Management Server Upgrade Guide

This Upgrade Guide describes how to migrate from Symantec Encryption Management Server version 3.3.2 or later to version 10.5 and how to migrate a cluster to version 10.5.

Symantec Encryption Management Server 10.5 is based on CentOS 7.x. Therefore, you must back up and restore the Symantec Encryption Management Server version 3.3.2 or later data to migrate to version 10.5 (or later).

**Warning:** PUP update is not supported when you migrate from Symantec Encryption Management Server 3.3.2 or later to Symantec Encryption Management Server 10.5 (or later).

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.

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 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.
- 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 the Symantec Encryption Management Server online help by clicking the online help icon in the upper-right corner of the Symantec Encryption Management Server screen.
- Symantec Encryption Management Server release notes is also provided, which may have last-minute information not found in the product documentation.

## Technical Support

For information about Symantec Enterprise Security Support, visit our website at the following URL:

https://support.broadcom.com/security

# 2 About Upgrading Symantec Encryption Management Server

This chapter describes how to migrate versions 3.3.2 or later of the product to version 10.5 for a single, non-clustered, server.

Warning: If you have added a Hardware Token Ignition Key in your existing Symantec Encryption Management Server, you must add a Soft-Ignition Passphrase Ignition Key, and then delete the Hardware Token Ignition Key, before you migrate to version 10.5.

## Overview of the Upgrade Process

When you upgrade to Symantec Encryption Management Server 10.5:

- You can only migrate from Symantec Encryption Management Server 3.3.2 or later.
- You must use migration to upgrade. Migration is the method by which you back up data to an external location, install the new software version on a new server from an ISO file, and restore your data.
- If you have performed the Complete Customization method to customize Symantec Encryption Web Email Protection, back up and delete the customization template before you upgrade. When the upgrade is complete, create a new Complete Customization template for Symantec Encryption Web Email Protection. You cannot restore the complete customization template after you upgrade to Symantec Encryption Management Server 10.5. If you have performed the Advanced Customization method to customize Symantec Encryption Web Email Protection, back up your advanced customization templates before you upgrade. When the upgrade is complete, restore the advanced customization templates. For information about backing up and restoring your Symantec Encryption Web Email Protection customization templates, see https://knowledge.broadcom.com/external/article?legacyId=howto110292.

You can upgrade your Symantec Encryption Management Server to version 10.5 through the following method:

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

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.

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

- Before you migrate to Symantec Encryption Management Server 10.5, you must back up your data and your Organization Key to an external location.

---

**Caution**: To upload and restore backups of 2 GB or larger through the Symantec Encryption Management Server Web interface, you need to contact Technical Support. For information on restoring Encryption Management Server backups larger than 2 GB, see https://knowledge.broadcom.com/external/article?legacyId=TECH149146.

---

- You can migrate to Symantec Encryption Management Server 10.5 from version 3.3.2 or later only.
- If your current server is running Symantec Encryption Management Server version earlier than 3.3.2, then first upgrade to version 3.3.2 or later. And then migrate to Symantec Encryption Management Server 10.5 (or later).

# Before you update your Symantec Encryption Management Server to 10.5

Ensure that you read the instructions mentioned as follows before you update Symantec Encryption Management Server to 10.5 (or later):

- Read the best practices mentioned in the *Best Practices for Upgrade* (see "*Best Practices for an Upgrade*" on page 9) section.
- Use the Migration method to upgrade Symantec Encryption Management Server, and follow the instructions mentioned in the *Migrating your Symantec Encryption Web Email Protection Complete Customizations* (on page 16) section for updating your Symantec Encryption Web Email Protection Complete Customization.
- Install the Symantec Encryption Management Server software on Symantec Encryption Management Server Certified Hardware. For more details refer to the "Symantec Encryption Management Server Certified Hardware List" section in the *System requirements for Symantec Encryption Management Server 10.5*.

# Best Practices for an Upgrade

The information in this list helps to 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.

**Important:** 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 a Message Transfer Agent (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 routes 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.

### Upgrading your Communications Network

Symantec Encryption Management Server 10.5 supports TLS 1.2 secure communication with clients running version 10.5 of Symantec Encryption Desktop and PGP Command Line. To maximize the use of this highly secure communications protocol, consider making a communications upgrade part of your upgrade to version 10.5.

Specifics of this functionality are:

- Clients can connect to all services on Symantec Encryption Management Server using TLS 1.2.
- When clients connect that are running previous versions of Symantec Encryption Desktop or PGP Command Line, the Management Server continues to support TLS 1.0 for backward compatibility.
- The Management Server connects to other servers, such as Directory Servers, Key Servers, and Email servers, using TLS 1.2. The Management Server also adjusts to the highest TLS version that a remote server supports. For example, if the remote server supports only TLS 1.0, then the Management Server makes the connection using TLS 1.0.
- Clients running v 10.4 of Symantec Encryption Desktop and PGP Command Line exhibit similar behavior to the Management Server when connecting to Key Servers or LDAP servers, when doing key searches.
- Note that when an e-Token is used during enrollment, the Symantec Encryption Desktop client still authenticates using TLS 1.0. After enrollment, the client uses TLS 1.2 for all further communications.

To migrate your data from version 3.3.2 or later to Symantec Encryption Management Server version 10.5, 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 3.3.2 backup file is 1 GB, you should have 10 GB of disk space to allow for the migration and expansion of your data into the 10.5 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 10.5.

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 10.5, 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 migrate, 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, select **Keys > Organization Keys**.
2. Click **Organization Key**.
3. Click **Export**.
4. Select **Export Keypair** and type a 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**.

# Upgrading Your Symantec Encryption Management Server to Version 10.5

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

To migrate from version 3.3.2 or later to version 10.5 (or later)

**Note:** You can migrate to Symantec Encryption Management Server version 3.4.0 or later from versions 3.3.2 or later. First upgrade your server version earlier than 3.3.2 to 3.3.2 or later before you migrate the server to version 10.5 (or later). For more details to upgrade from earlier versions of Symantec Encryption Management Server to 3.3.2, see the *Symantec Encryption Management Server Upgrade Guide 10.5*.

1. Log on to your Symantec Encryption Management Server version 3.3.2 or later administrative interface.
2. Back up your Symantec Encryption Management Server 3.3.2 or later data to a remote location, such as FTP or SCP backup.
3. Perform a fresh install of Symantec Encryption Management Server 10.5 (or later) on the system.

   **Note:** If you are installing the Symantec Encryption Management Server 3.4.0 or later on a new system and if you want to use the IPs of the older system on which 3.3.2 or later server was installed, then deactivate this older system.
4. Restore your Organization Key and data.

## 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 the migration method to upgrade your Symantec Encryption Management Server.

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.

Note: During 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 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 the **Export...** button at the bottom of the screen.
6. Select the log file or schema report you wish to download.

## Running the 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`

### Supported Client and Symantec Encryption Management Server Version Combinations

Symantec supports backward compatibility for clients only. Symantec Encryption Management Server 10.5 supports managing policies of these client versions only:

- Symantec Encryption Desktop 10.3.2 and later Maintenance Packs
- Symantec Encryption Desktop 10.4.0 and later Maintenance Packs

Note: 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.

## 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 10.5.

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) are 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.
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*.

When you back up data on one Symantec Encryption Management Server and then restore the data to another Symantec Encryption Management Server, the MAC address of the restored server is set to the MAC address of the backed up Symantec Encryption Management Server. This issue cannot be fixed through the administrative interface of the server. This issue is corrected via the command line of the Symantec Encryption Management Server by editing the hostname, IP address, gateway, MAC address, and netmask fields in the prefs.xml file.

## Migrating your Symantec Encryption Web Email Protection Complete Customizations

- **Note:** If you have performed the Complete Customization method to customize Symantec Encryption Web Email Protection, back up and delete the customization template before you upgrade. When the upgrade is complete, create a new Complete Customization template for Symantec Encryption Web Email Protection. You cannot restore the complete customization template after you upgrade to Symantec Encryption Management Server 10.5. If you have performed the Advanced Customization method to customize Symantec Encryption Web Email Protection, back up your advanced customization templates before you upgrade. When the upgrade is complete, restore the advanced customization templates. For information about backing up and restoring your Symantec Encryption Web Email Protection customization templates, see https://knowledge.broadcom.com/external/article?legacyId=howto110292.

Before migrating Symantec Encryption Management Server to version 10.5 (or later) using the backup and restore method, you must perform the following steps for updating your Symantec Encryption Web Email Protection Complete Customization:

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

2 In the **Customization** panel, select **Complete Customization** and click the **Download Customization file** option next to it.

3 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.

After you have migrated your server to version 3.4.0 or later, perform the following steps for updating your Symantec Encryption Web Email Protection Complete Customization:

1 Zip the locally updated files.

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

The other fields are optional.

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

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

Note: When you upgrade to Symantec Encryption Management Server 10.5 (or later) from a 3.3.2 version, the Password Reveal Button features of the Internet Explore 10 or later for Web Email Protection users is not supported. Also, when you perform a backup and restore from a 3.3.2 version of your server to Symantec Encryption Management Server 10.5, this feature is disabled by default. You must manually configure this setting after upgrade. For more information, see the section *Configuring Symantec Encryption Web Email Protection* available in the Symantec Encryption Management Server online help.

## How Upgrading Affects Mail Policy Settings

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

- **Fresh Installation:** If you migrate 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 10.5.

For an overview of clustering in Symantec Encryption Management Server version 10.5, see *Clustering your Symantec Encryption Management Servers* in the *Symantec Encryption Management Server Administrator's Guide*.

Upgrade each server cluster member individually. See section *Upgrading Your Symantec Encryption Management Server to Version 10.5* (on page 11) to follow the migration instructions, depending on the Symantec Encryption Management Server version that you want to upgrade from.

**Important:** You do not need to remove the member from the cluster before upgrading.

**Note:** When you are migrating your cluster members from Symantec Encryption Management Server version earlier than 3.3.2 to version 10.5 (or later), then you need to first upgrade your server version to 3.3.2 or later.

## Cluster Migration Overview

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

Your sponsoring server must be migrated first. As part of the backup restoration process, the sponsoring server's 3.3.2 or later data is migrated into the version 10.5 database. This server now acts as the sponsor for the other cluster members. As it is joined to the new 10.5 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 to each cluster member and is not replicated to other cluster members.

If there are data inconsistencies or conflicts between the version 10.5 sponsoring and its joining servers, the migration process may not be able to reconcile the inconsistencies. 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.

## 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 to version 10.5, you must be running version 3.3.2 or later. If you are running an earlier version, you must upgrade to version 3.3.2 or later on each server.

The upgraded and restored sponsoring 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* in this document.

**Note:** The migration process may not be able to reconcile data inconsistencies, and in some cases, inconsistent data from a joining server may be lost.

## Migrating Your Cluster

This process provides an overview of the cluster upgrade process.

1 Verify that your cluster members are running version 3.3.2 or later.

If your cluster members are running an earlier version, you must first upgrade to version 3.3.2 or later.

Inconsistent data may not migrate correctly to version 10.5.

2 Back up all cluster members that have server version 3.3.2 or later installed to an external location.

**Note:** You should back up each joining sever if the original cluster was in the "Home Server" or "Replicated on <x> out of the <y> servers in the cluster" mode. In the "High Availability" mode, you should back up only the sponsoring server.

You must first update your sponsoring and joining servers to version 3.3.2 before migrating to Symantec Encryption Management Server 10.5 (or later). For more information, see *Upgrading Your Symantec Encryption Management Server to Version 10.5* in this document.

For more information on backing up your Symantec Encryption Management Servers, including their Organization Keys, see *Backing Up the Data and Organization Key* in this document.

3 Perform a fresh install of Symantec Encryption Management Server 10.5 on your sponsoring server.

See *Upgrading Your Symantec Encryption Management Server to Version 10.5* in this document 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 sponsoring server's administrative interface to see the previous joining servers that are listed as pending cluster members.

4 Perform a fresh install of Symantec Encryption Management Server 10.5 on each joining server.

**Note:** You must first update your server to version 3.3.2 before migrating to Symantec Encryption Management Server 10.5.

5 Restore each joining server's backup before you join the joining servers to the new cluster.

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

You should restore the back up of the joining sever if the original cluster was in the "Home Server" or "Replicated on <x> out of the <y> servers in the cluster" mode. In the "High Availability" mode, you should restore the back up of only the sponsoring server because all cluster members share the same user data. It is always faster to update the sponsoring server and then join the joining servers.

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

6 (Optional) If you have removed the members from the cluster before upgrading, then do the following:

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

b Type the IP address of the previous sponsoring server, which is now the sponsor server.

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

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

This step initiates the join and the data replication process. For more information on migrating your sponsoring and joining cluster members, see *Migrating your Sponsoring Cluster Server* (on page 21) and *Migrating a Joining Cluster Member* (on page 23).

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.

# Migrating your Sponsoring Cluster Server

Before you migrate, ensure that your cluster members are running version 3.3.2 or later.

To migrate your sponsoring cluster

1 Download, install, and configure the Symantec Encryption Management Server version 10.5.

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

For detailed information see *Backing Up the Data and Organization Key* in this document.

3 Follow the instructions in *Upgrading Your Symantec Encryption Management Server to Version 10.5* to migrate your sponsoring server to Symantec Encryption Management Server 10.5 that you have configured in step 1.

For more information on installing 10.5 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 sponsoring 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 sponsoring server.

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

Until the joining servers rejoin the cluster, their status remains as pending. The join action must be requested by each former joining server. The **Contact** button that appears next to each pending member does not have an effect until the former joining 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 joining server has been migrated to version 10.5 and has requested a join, in the sponsoring server's administrative interface, select **System** > **Clustering**.

7 Click **Contact** next to the joining server 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 joining server. For example, if your cluster was previously running Symantec Encryption Web Email Protection in the Home Server mode, the join process migrates all Web Email Protection data that was kept on the joining server. 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 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 joining server 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 Joining Cluster Member

To migrate a joining cluster member

This procedure provides instructions to migrate your joining cluster members.

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

For more information, see *Backing Up the Data and Organization Key* (on page 11).

2 Follow the instructions in *Upgrading Your Symantec Encryption Management Server to Version 10.5* to migrate your joining server to Symantec Encryption Management Server version 10.5.

Detailed instructions on installing the 10.5 software and running the Setup Assistant are found in the *Symantec Encryption Management Server Installation Guide*.

3 Restore the backup.

You should only restore the back up on the joining servers when your cluster is running Web Email Protection in the Home Server mode. Otherwise, it is always more efficient to install Symantec Encryption Management Server 10.5 on the joining 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 joining server under these conditions:

- You are running Symantec Encryption Web Email Protection in the Home Server mode or Web Email Protection was not running on this server.

- You did not preserve server-specific settings for mail routes, mail proxies, or external LDAP servers.
- You did not restore the SSL/TSL certificate for this joining server.

For more information, see *Manually Reconfiguring Non-replicated Server Settings* (on page 24).

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

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

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

6 The sponsoring server initiates the join and data replication.

7 Monitor the progress bar to track the replication.

Repeat these steps to migrate and rejoin all your former joining servers to the version 10.5 cluster. We recommend that you always use the former sponsoring server as the sponsor server.

## Manually Reconfiguring Non-Replicated Server Settings

If you do not plan to restore the backup onto a joining server, but would like to preserve some non-replicated settings, you can individually restore those settings after you migrate to 3.4.2.

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

a On each joining 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 must re-configure these settings on the joining server after you install 3.4.2.

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 Symantec Encryption Management Server 10.5 on your former joining server, and **before** you join this server to the new 10.5 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 joining server, you must restore the full backup.

1. If your joining server used a different SSL/TLS certificate from the former sponsoring server, import the certificate you exported in step 1c in the 'save specific, non-replicated settings procedure.'

   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 10.5, 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)
- Replicated on <x> out of the <y> servers in the cluster

  You can 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.

- Not replicated (as in the former HS mode).

Note: In a cluster setup, you cannot have the Password Reveal Button setting replicated to all Symantec Encryption Management Servers in a cluster that are running the Symantec Encryption Web Email Protection service. To replicate the settings, execute the following command:

```
# pgprepctl file /etc/ovid/prefs.xml
```

Re-execute this command after each modification of the prefs.xml file to replicate the settings on all servers across the cluster.

# Index