



## Complete the Replacement

---

- [Create Backup, page 1](#)
- [Obtain License File, page 5](#)
- [Verify NTP Status, page 5](#)
- [Install Software on Publisher Server, page 5](#)
- [Install Software on Subscriber Server, page 8](#)
- [Upload License File, page 10](#)
- [Restore Backup File, page 11](#)
- [Complete Replacement, page 13](#)

## Create Backup

The following sections describe how to set up and run a backup before an upgrade. Refer to the *Administration Guide for Cisco Unified Communications Manager* for more information.

If you are recovering or replacing a server, you can skip this section on creating backups and restore the server from the most recent backup that is available.

### Related Topics

[Replace Publisher Node](#)

[Replace Subscriber or Dedicated TFTP Server](#)

## Supported Features and Components

You can back up and restore the features and subcomponents that are shown in the following table. For each feature that you choose, the system backs up all its subcomponents automatically.

**Table 1: Supported Features and Components**

Feature	Components
CCM - Cisco Unified Communications Manager	Cisco Unified Communications Manager database (CMDB)
	Platform
	Cisco Unified Serviceability
	Music On Hold (MOH)
	Cisco Emergency Responder (CER)
	Bulk Tool (BAT)
	Preference
	Phone device files (TFTP)
	syslogagt (SNMP syslog agent)
	cdpagent (SNMP cdp agent)
	tet (trace collection tool)
	Call Detail Records (CDR)
	CDR Analysis and Reporting (CAR)

## Configure Features for Backup

Before you can schedule or start a backup job, you must configure the features that you want to back up.



**Note** Changing a backup feature changes it for both manual and scheduled backups.

Perform the following steps to choose the features that you want to back up.

### Procedure

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose Disaster Recovery System from the Navigation menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**. The Disaster Recovery System Logon window displays.

- Step 2** Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup > Configure Features**.
- Step 4** From the list of available features, choose the feature or features that you want to include in the backup and click **Save**. You must choose at least one feature.
- Step 5** Continue with the next procedure for configuring a storage location.
- 

## Configure Storage Location

Before using the Disaster Recovery System, you must configure the location where you want the backup file to be stored. Perform the following steps to configure the storage location.

### Procedure

---

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**. The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup > Storage Location**. The Storage Location window displays.  
**Note** You can configure the number of backup sets that are stored on a network directory.
- Step 4** Select the Network Directory option to store the backup data on a networked drive that is accessed through an SFTP connection.
- Step 5** Enter the following required information:
- Server name: Name or IP address of the network server
  - Path name: Path name for the directory where you want to store the backup file
  - User name: Valid username for an account on the remote system
  - Password: Valid password for the account on the remote system
- Note** You must have access to an SFTP server to configure a network storage location. The SFTP path must exist prior to the backup. Ensure that the account that is used to access the SFTP server has write permission for the selected path.
- Step 6** To update these settings, click **Save**.  
**Note** For network directory backups, after you click the Save button, the DRS Master Agent will validate the selected SFTP server. If the user name, password, server name, or directory path is invalid, the save will fail.
- Step 7** Continue with either a manual or a scheduled backup.
-

## Start Backup

You can manually start a backup of the features that you choose on the Configure Features menu. Perform the following steps to start a manual backup.

### Procedure

---

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.  
The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup > Manual Backup**. The Manual Backup window displays.
- Step 4** Make sure the features that you want to back up are chosen. To choose other features, see the [Configure Features for Backup, on page 2](#).
- Note** Ensure all servers in the cluster are running the same version of Cisco Unified Communications Manager and are reachable through the network. Servers that are not running at the time of the scheduled backup will not get backed up.
- Step 5** To begin the manual backup, click **Start Backup**.
- Step 6** Make sure that you have configured the backup storage location. See the [Configure Storage Location, on page 3](#).
- 

## Check Backup Status

Perform the following steps to check the status of the current backup job.

### Procedure

---

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.  
The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Backup > Current Status**. The Backup Status window displays.
- Step 4** To view the backup log file, click the log filename link.
- Step 5** To cancel the current backup, click **Cancel Backup**.
- Note** The backup cancels after the current component completes its backup operation.
-

## Obtain License File

If you have to replace the first node in your Cisco Unified Communications Manager cluster, you must open a case with the licensing team to obtain a license for your replacement server. Contact the licensing team at [licensing@cisco.com](mailto:licensing@cisco.com). After you receive the new license file, upload the software license file.



---

**Note** Replacing a motherboard on the first node also requires a new license file.

---

### Related Topics

[Upload License File, on page 10](#)

[Replace Publisher Node](#)

## Verify NTP Status

If you are getting the system time from an NTP server, verify that the publisher node can synchronize with the NTP server before you install a subscriber node.

To verify the NTP status of the first node, log into the command line interface on the publisher node and enter the following command:

```
utils ntp status
```

For more information, see the *Cisco Unified Communications Command Line Interface Guide*.



---

**Caution** If the first node fails to synchronize with an NTP server, installation of a subsequent node can also fail.

---

## Install Software on Publisher Server

Use this procedure to install Cisco Unified Communications Manager on the new publisher server. For more information about installing this product, refer to the document, *Installing Cisco Unified Communications Manager*.

### Procedure

---

- Step 1** Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.
- Step 2** To perform the media check, choose **Yes** or, to skip the media check, choose **No**. The media check checks the integrity of the DVD. If your DVD passed the media check previously, you might choose to skip the media check.
- Step 3** If you choose **Yes** to perform the media check, the system installer performs the media check and displays the Media Check Result window. Perform these tasks:

- a) If the Media Check Result displays Pass, choose **OK** to continue the installation.
- b) If the media fails the media check, either download another copy of the software from Cisco.com or obtain another disc directly from Cisco.

**Step 4** In the Product Deployment Selection window, select Cisco Unified Communications Manager; then, choose **OK**.

**Step 5** If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. To continue with the installation, choose **Yes**, or choose **No** to cancel.

**Caution** If you choose **Yes** on the Overwrite Hard Drive window, all existing data on your hard drive gets overwritten and destroyed.

**Step 6** The Platform Installation Wizard window displays.

**Step 7** To configure the platform now, choose **Proceed**.

**Step 8** In the Basic Install window, choose **Continue** to install the software version on the DVD.

**Step 9** When the Timezone Configuration displays, choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

**Step 10** The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.

- To enable automatic negotiation, choose **Yes**.

The MTU Configuration window displays.

**Note** To use this option, your hub or Ethernet switch must support automatic negotiation.

- To disable automatic negotiation, choose **No** and continue with the next step.

The NIC Speed and Duplex Configuration window displays.

**Step 11** If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.

The MTU Configuration window displays.

**Step 12** In the MTU Configuration window, you can change the MTU size from the operating system default. The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.

**Caution** Configuring the MTU size incorrectly can affect your network performance.

- To accept the default value (1500 bytes), choose **No**.
- To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK**.

The DHCP Configuration window displays.

**Step 13** For network configuration, you can choose to either set up static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP).

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**.

The Administrator Login Configuration window displays.

- If you want to configure static IP address for the node, choose **No** and continue with the next step.

The Static Network Configuration window displays.

**Step 14** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See [Record Network Configuration Settings](#) for field descriptions.

The DNS Client Configuration window displays.

**Step 15** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See [Record Network Configuration Settings](#) for field descriptions.

The Administrator Login Configuration window displays.

**Step 16** Enter your Administrator login and password from [Account Names and Passwords Record](#).

The Certificate Signing Request Information window displays.

**Step 17** Enter your certificate signing request information and choose **OK**.

The First Node Configuration window displays.

**Step 18** To configure this server as the first Cisco Unified Communications Manager node, choose **Yes**.

The Network Time Protocol Client Configuration window displays.

**Step 19** Choose whether you want to configure an external NTP server or manually configure the system time.

**Note** Cisco recommends that you use an external NTP server to ensure accurate system time on the first node. Ensure the external NTP server is stratum 9 or higher (meaning stratum 1-9). Subsequent nodes in the cluster will get their time from the first node.

- To set up an external NTP server, choose **Yes** and enter the IP address, NTP server name, or NTP server pool name for at least one NTP server. You can configure up to five NTP servers, and Cisco recommends that you use at least three. Choose **Proceed** to continue with the installation.

The system contacts an NTP server and automatically sets the time on the hardware clock.

**Note** If you already entered the network configuration information and the system rebooted (a Skip installation), the **Test** button displays. You can choose **Test** to check whether the NTP servers are accessible.

- To manually configure the system time, choose **No** and enter the appropriate date and time to set the hardware clock. Choose **OK** to continue with the installation.

The Database Access Security Configuration window displays.

**Step 20** Enter the Database Access Security password from [Account Names and Passwords Record](#).

The SMTP Host Configuration window displays.

**Step 21** If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

**Note** You must configure an SMTP server to use certain platform features; however, you can also configure an SMTP server later by using the operating system GUI or the command line interface.

**Step 22** Choose **OK**.

The Platform Configuration Confirmation window displays.

**Step 23** To continue with the installation, choose **OK**.

The Application User Password Configuration window displays.

**Note** If you need to change one of your previous entries, choose **Back**, make the change, and continue with the installation.

- Step 24** Enter the Application User Password from [Account Names and Passwords Record](#) and confirm the password by entering it again.
- Step 25** Choose **OK**.  
The system installs and configures the software. The DVD drive ejects, and the server reboots. Do not reinsert the DVD.
- Step 26** When the installation process completes, you get prompted to log in by using the Administrator account and password.
- Step 27** Complete the rest of the tasks that are listed in the [Replace Publisher Node](#).
- 

## Install Software on Subscriber Server

Use this procedure to install Cisco Unified Communications Manager on a new subscriber server.

### Procedure

---

- Step 1** If you configured Network Time Protocol (NTP) on the publisher node, ensure that the publisher node is synchronized with an NTP server before you install a subscriber node. From the Command Line Interface on the publisher node, enter the command `utils ntp status`. Ensure that the printout indicates that the node is synchronized with an NTP server.
- Note** If the first node is not synchronized with an NTP server, installation of the subsequent node will fail.
- Step 2** Insert the installation DVD into the tray and restart the server, so it boots from the DVD. After the server completes the boot sequence, the DVD Found window displays.
- Step 3** To perform the media check, choose **Yes** or, to skip the media check, choose **No**.  
The media check checks the integrity of the DVD. If your DVD has passed the media check previously, you might choose to skip the media check.
- Step 4** If you choose **Yes** to perform the media check, the system installer performs the media check and displays the Media Check Result window. Perform these tasks:
- If the Media Check Result displays Pass, choose **OK** to continue the installation.
  - If the media fails the media check, either download another copy of the software from Cisco.com or obtain another disc directly from Cisco.
- Step 5** In the Product Deployment Selection window, select Cisco Unified Communications Manager; then, choose **OK**.
- Step 6** If software is currently installed on the server, the Overwrite Hard Drive window opens and displays the current software version on your hard drive and the version on the DVD. Choose **Yes** to continue with the installation or **No** to cancel.
- Caution** If you choose Yes on the Overwrite Hard Drive window, all existing data on your hard drive gets overwritten and destroyed.

- Step 7** The Platform Installation Wizard window displays.
- Step 8** To configure the platform now, choose **Proceed**.
- Step 9** In the Basic Install window, choose **Continue** to install the software version on the DVD.
- Step 10** When the Timezone Configuration displays, choose the appropriate time zone for the server and then choose **OK**.  
The Auto Negotiation Configuration window displays.
- Step 11** The installation process allows you to automatically set the speed and duplex settings of the Ethernet network interface card (NIC) by using automatic negotiation. You can change this setting after installation.
- To enable automatic negotiation, choose **Yes**.  
The MTU Configuration window displays.  
**Note** To use this option, ensure that your hub or Ethernet switch supports automatic negotiation.
  - To disable automatic negotiation, choose **No** and continue with the next step.  
The NIC Speed and Duplex Configuration window displays.
- Step 12** If you chose to disable automatic negotiation, manually choose the appropriate NIC speed and duplex settings now and choose **OK** to continue.  
The MTU Configuration window displays.
- Step 13** In the MTU Configuration window, you can change the MTU size from the operating system default. The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.
- Caution** Configuring the MTU size incorrectly can affect your network performance.
- To accept the default value (1500 bytes), choose **No**.
  - To change the MTU size from the operating system default, choose **Yes**, enter the new MTU size, and choose **OK**.
- The DHCP Configuration window displays.
- Step 14** For network configuration, you can choose to either set up static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP).
- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**.  
The Administrator Login Configuration window displays.
  - If you want to configure static IP address for the node, choose **No** and continue with the next step.  
The Static Network Configuration window displays.
- Step 15** If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See [Record Network Configuration Settings](#) for field descriptions.  
The DNS Client Configuration window displays.
- Step 16** To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See [Record Network Configuration Settings](#) for field descriptions.  
The Administrator Login Configuration window displays.

- Step 17** Enter your Administrator login and password from [Account Names and Passwords Record](#). The Certificate Signing Request Information window displays.
- Step 18** Enter your certificate signing request information and choose **OK**. The First Node Configuration window displays.
- Step 19** To configure this server as a subsequent node in the cluster, choose **No**. The First Node Configuration window displays.
- Caution** You must configure a subsequent node on the first node by using Cisco Unified Communications Manager Administration before you install the subsequent node. For more information, see the *Administration Guide for Cisco Unified Communications Manager*.
- Step 20** On the First Node Configuration window, read the Warning and make sure that you have correctly configured the first node. To continue with the installation of the subsequent node, choose **OK**. The Network Connectivity Test Configuration window displays.
- Step 21** During installation of a subsequent node, the system checks to ensure that the subsequent node can connect to the first node.
- To pause the installation after the system successfully verifies network connectivity, choose **Yes**.
  - To continue the installation with a pause, choose **No**.
- The First Node Access Configuration window displays.
- Step 22** Enter the first node connectivity information to enable this subscriber node to connect to the subscriber node. If you chose to pause the system after the system successfully verified network connectivity, the Successful Connection to First Node window displays. Choose **Continue**.
- Note** If the network connectivity test fails, the system always stops and allows you to go back and reenter the parameter information. The SMTP Host Configuration window displays.
- Step 23** If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.
- Note** You must configure an SMTP server to use certain operating system features; however, you can also configure an SMTP server later by using the operating system GUI or the command line interface. The Platform Configuration Confirmation window displays.
- Step 24** To start installing the software, choose **OK**, or if you want to change the configuration, choose **Back**.
- Step 25** When the installation process completes, you get prompted to log in by using the Administrator account and password.
- Step 26** Complete the rest of the tasks in the [Replace Subscriber or Dedicated TFTP Server](#).
- 

## Upload License File

Use the following procedure to upload a license file to the Cisco Unified Communications Manager server with the matching MAC address that is provided when a license file is requested. For information about obtaining a license file, see the [Obtain License File](#), on page 5. The Cisco Unified Communications Manager server where the license file is loaded takes on the functionality of the license manager.



---

**Note** Upload the license file only on the first node of Cisco Unified Communications Manager cluster.

---

### Procedure

---

- Step 1** Choose **System > License > Upload License File**.  
The License File Upload window displays.
- Step 2** The Existing License Files drop-down list box displays the license files that are already uploaded to the server.  
**Note** To view the file content of any existing files, choose the file from the drop-down list box and click **View File**.
- Step 3** To choose a new license file to upload, click **Upload License File**.  
The Upload File window displays.
- Step 4** Browse and choose a license file to upload to the server.  
**Note** The format of the license file that you receive specifies CCM<timestamp>.lic. If you retain the .lic extension, you can rename the license file. You cannot use the license if you edit the contents of the file in any way.
- Step 5** Click **Upload License File**.  
After the upload process completes, the Upload Result file displays.
- Step 6** Click **Close**.
- Step 7** In the License File Upload window, the status of the uploaded file displays.  
**Note** The system uploads the license file into the database only if the version that is specified in the license file is greater than or equal to the Cisco Unified Communications Manager version that is running in the cluster. If the version check fails, an alarm occurs, and you should get a new license file with the correct version. The system bases the version check only on major releases.
- Step 8** Restart the Cisco CallManager service. For information on restarting services, refer to the *Administration Guide for Cisco Unity Connection Serviceability*.
- 

### Related Topics

[Replace Publisher Node](#)

## Restore Backup File

The Restore Wizard takes you through the steps that are required to restore a backup file. To perform a restore, use the procedure that follows.



### Caution

---

Before you restore Cisco Unified Communications Manager, ensure that the Cisco Unified Communications Manager version that is installed on the server matches the version of the backup file that you want to restore.

---

## Procedure

---

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.  
The Disaster Recovery System Logon window displays.
- Step 2** Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.
- Step 3** Navigate to **Restore > Restore Wizard**. The Restore Wizard Step 1 window displays.
- Step 4** Choose the Network Directory storage location from which you want to restore the file and enter the following required information for the chosen storage location:
- Server name: Name or IP address of the network server
  - Path name: Path name for the directory from which you want to restore the backup data
  - User name: Valid username for an SFTP account on the remote system
  - Password: Valid password for the SFTP account on the remote system
- Step 5** Click **Next**. The Restore Wizard Step 2 window displays.
- Step 6** Choose the backup file that you want to restore.  
**Note** The backup filename indicates the date and time that the system created the backup file.
- Step 7** Click **Next**. The Restore Wizard Step 3 window displays.
- Step 8** Choose the features that you want to restore.  
**Note** Only the features that were backed up to the file that you chose display.
- Step 9** Click **Next**. The Restore Wizard Step 4 window displays.
- Step 10** To start restoring the data, click **Restore**.  
You get prompted to choose the node to restore.
- Step 11** Choose the appropriate node.  
**Caution** After you choose the node to which you want the data restored, any existing data on that server gets overwritten.
- Step 12** Your data gets restored on the nodes that you chose.  
**Note** Depending on the size of your database and the components that you choose to restore, the system can require 1 hour or more to restore.
- 

## Related Topics

- [Replace Publisher Node](#)
- [Replace Subscriber or Dedicated TFTP Server](#)
- [View Restore Status, on page 13](#)

## View Restore Status

To check the status of the current restore job, perform the following steps:

### Procedure

---

- Step 1** Navigate to the Disaster Recovery System. Log in to Cisco Unified Communications Manager Administration, choose **Disaster Recovery System** from the **Navigation** menu in the upper, right corner of the Cisco Unified Communications Manager Administration window, and click **Go**.  
The Disaster Recovery System Logon window displays.
  - Step 2** Log in to the Disaster Recovery System by using the same Administrator user name and password that you use for Cisco Unified Communications Operating System Administration.
  - Step 3** Navigate to **Restore > Status**. The Restore Status window displays.
  - Step 4** To view the restore log file, click the log filename link.
- 

## Complete Replacement

Perform the following tasks after you complete the cluster replacement:

### Procedure

---

- Step 1** If your server or cluster ran in secure mode, create a new CTL file and distribute it to all the cluster nodes. Do this step after you finish replacing or reinstalling all the servers that you intend to replace or reinstall. For information about performing these tasks and about Cisco Unified Communications Manager security, refer to the *Cisco Unified Communications Manager Security Guide*.  
**Caution** You must create and distribute a new CTL file, or your secure phones will not work because they cannot register with the replaced Cisco Unified Communications Manager server(s).
- Step 2** Using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), make sure that all the registration information values match the values that you recorded before the server replacement.
- Step 3** Using the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), make sure that all the critical services and their status match those that you recorded before the server replacement.
- Step 4** Using the Syslog viewer in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), locate any events that have a severity of Error or higher. Perform this task to ensure that no system-affecting errors exist on your system.
- Step 5** Using the Syslog viewer in the Cisco Unified Communications Manager Real Time Monitoring Tool (RTMT), check the Replicate\_State counter for the Number of Replicates Created and State of Replication object on all nodes. The value on each node should equal 2.  
This counter represents the state of replication, which includes the following possible values:
  - 0 - Initializing. The counter equals 0 when the server is not defined or when the server is defined but the realize template has not completed.

- 1 - The system created replicates of some tables but not all tables. Cisco recommends that you run `utils dbreplication status` on the CLI to determine the location and cause of the failure.
- 2 - Good Replication.
- 3 - Bad Replication. When the counter displays a value of 3, consider replication in the cluster as bad. It does not mean that replication failed on a particular node. Cisco recommends that you run `utils dbreplication status` on the CLI to determine the location and cause of the failure.
- 4 - Replication setup did not succeed.

**Step 6** To access the appropriate object and counter, use the following procedure:

a) Perform one of the following tasks:

- In the Quick Launch Channel, click **System > Performance**; then, click the **Performance** icon.
- Choose **Performance > Open Performance Monitoring**.

b) Double-click the name of the server where you want to add a counter to monitor.

c) Double-click the **Number of Replicates Created** and **State of Replication** object.

d) Double-click the **Replicate\_State** counter.

e) Choose the **ReplicateCount** instance and click **Add**.

**Step 7** From Cisco Unified Communications Manager Administration, make sure that the number of phones, gateways, trunks, users, and route patterns that are configured in the database matches the numbers that you recorded before the server replacement.

**Step 8** From the Firmware Load Information window in Cisco Unified Communications Manager Administration, make sure that the phone load type value matches the value that you recorded before the server replacement.

**Step 9** Reinstall the COP file enablers for any custom device types that do not ship with Cisco Unified Communications Manager. Then, reboot the cluster and start post-replacement checklist again.

**Step 10** Reinstall any locales that were installed on the server.

**Step 11** Compare the system version on each node in your cluster by using Cisco Unified Communications Operating System Administration and make sure that it matches the version that you recorded before the replacement.

**Step 12** Reconfigure CDR destinations, if applicable.

**Step 13** Reconfigure all Trace and Log Central jobs.

**Step 14** Perform any system tests that you performed before the replacement and verify that all test calls succeed.

**Step 15** Reconfigure DRS location and schedule, if applicable.

## Related Topics

- [Record System Configuration Counts](#)
- [Determine Registration Counts](#)
- [Record Critical Services](#)
- [Locate System Errors](#)
- [Record Firmware Information](#)
- [Record System Version](#)
- [Record CDR Management Configuration](#)
- [Record Trace Log Job Details](#)

[Create Backup, on page 1](#)

