Installing Cisco Unified Communications Manager Release 8.6(1)

Revised: 12/11/2012

This document includes information about installing Cisco Unified Communications Manager release 8.6(1). Review all installation instructions carefully before you install Cisco Unified Communications Manager.

This document includes information about installing Cisco Unified Communications Manager Release 8.6(1) on one server or many servers in a cluster environment.

For information about upgrading from a previous release of Cisco Unified Communications Manager, and for other installation and upgrade information, see the "Related Documentation" section on page 2.

Contents

This document contains the following topics:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Related Documentation

For additional installation and upgrade information, refer to the following documents:

- *Upgrading Cisco Unified Communications Manager*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

  This document describes how upgrade Cisco Unified Communications Manager from Release 6.1(2) and later.

- *Cisco Unified Communications Operating System Administration Guide*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

  This document describes how to upgrade Cisco Unified Communications Manager to a later appliance-based release.

- *Replacing a Single Server or Cluster for Cisco Unified Communications Manager*

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

  This document describes how to replace a Cisco Unified Communications Manager server or a cluster of servers.

- *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions* http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

This document describes the Command Line Interface for Cisco Unified Communications Manager. Some of these commands perform upgrade and installation-related tasks.

For further information about Cisco Unified Communications Manager documentation, refer to the following URL:

http://cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html.

Table 1 lists URLs for software and additional documentation.

Table 1 Quick Reference for URLs

Related Information and Software	URL
Cisco MCS data sheets	http://www.cisco.com/en/US/products/hw/voiceapp/ps378/index.html
Cisco Unified Communications Manager service releases	http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Note The installation procedure is different for MCS 7825 H3 and MCS 7828 H3, when compared to other MCS servers that are mentioned in the Cisco MCS data sheets. For more information, see Step 5, Starting the Installation, page 23.

Installation Scenarios

You can use this document to perform the following different installation scenarios:

- Install software from a DVD on the first node
- Install software from a DVD on a subsequent node
- Apply a patch during installation of the first node
- Apply a patch during installation of a subsequent node
- Add a new node to an existing cluster
- Reusing the MCS-7828 After Installing Cisco Unified Communications Manager Business Edition 5000

The following sections provide an overview of the high-level tasks that you must perform for each of these installation scenarios. Each high-level task also includes a link to another section of the document, which you can follow for detailed information about the task.

Note For information about replacing a server or cluster, refer to *Replacing a Single Server or Cluster for Cisco Unified Communications Manager.*

Install Software from a DVD on the First Node

To install software that you have on a DVD on the first node in a cluster, follow the steps in Table 1.

Table 2 Installing Software from a DVD on the First Node

	Task	For More Information
Step 1	Perform all pre-installation tasks that apply to your site.	For a list of pre-installation tasks, see Table 1 on page 8.
Step 2	Follow the procedure to begin installing the software from the DVD to your server.	See the "Starting the Installation" section on page 23.
Step 3	Follow the procedure for performing a basic installation.	See the "Performing the Basic Installation" section on page 30.
Step 4	When the First Node Configuration window displays, choose **Yes** to configure the new server as the first node.	See Step 10 in the "Performing the Basic Installation" section on page 30.
Step 5	Follow the procedure to configure the first node.	See "Configuring the First Node" section on page 31
Step 6	Perform all post-installation tasks that apply to your site.	For a list of post-installation tasks, see Table 13 on page 34.

Install Software from a DVD on a Subsequent Node

To install software that you have on a DVD, follow the steps in Table 1.

Table 3 Installing Software from a DVD on a Subsequent Node

	Task	For More Information
Step 1	Perform all pre-installation tasks that apply to your site.	For a list of pre-installation tasks, see Table 1.
Step 2	Follow the procedure to begin installing the software from the DVD to your server.	See "Starting the Installation" section on page 23.
Step 3	Follow the procedure for performing a basic installation.	See "Performing the Basic Installation" section on page 30.
Step 4	When the First Node Configuration displays, choose **No** to configure the new server as a subsequent node.	See Step 10 in the "Performing the Basic Installation" section on page 30.
Step 5	Follow the procedure to configure a subsequent node in the cluster.	See the "Configuring a Subsequent Node" section on page 32.
Step 6	Perform all post-installation tasks that apply to your site.	For a list of post-installation tasks, see Table 13.

Apply a Patch During Installation of the First Node

You can upgrade to a later release by downloading and applying a patch during installation. To apply a patch during installation of the first node, follow the steps in Table 1.

Table 4 Applying a Patch During Installation of the First Node

	Task	For More Information
Step 1	Perform all pre-installation tasks that apply to your site.	For a list of pre-installation tasks, see Table 1.
Step 2	Follow the procedure to begin installing the software from the DVD to your server.	See "Starting the Installation" section on page 23.
Step 3	Follow the procedure to apply a software patch.	See "Applying a Patch" section on page 26.
Step 4	Follow the procedure for performing a basic installation.	See "Performing the Basic Installation" section on page 30.
Step 5	When the First Node Configuration window displays, choose **Yes** to configure the new server as the first node.	See Step 10 in the "Performing the Basic Installation" section on page 30.
Step 6	Follow the procedure to configure the first node in the cluster.	See the "Configuring the First Node" section on page 31.
Step 7	Perform all post-installation tasks that apply to your site.	For a list of post-installation tasks, see Table 13.

Apply a Patch During Installation of a Subsequent Node

You can upgrade to a later release by downloading and applying a patch during installation. To apply a patch during installation of a subsequent node, follow the steps in Table 1.

Table 5 Applying a Patch During Installation of a Subsequent Node

	Task	For More Information
Step 1	Perform all pre-installation tasks that apply to your site.	For a list of pre-installation tasks, see Table 1.
Step 2	Follow the procedure to begin installing the software from the DVD to your server.	See "Starting the Installation" section on page 23.
Step 3	Follow the procedure to apply a software patch.	See "Applying a Patch" section on page 26.
Step 4	Follow the procedure for performing a basic installation.	See "Performing the Basic Installation" section on page 30.
Step 5	When the First Node Configuration window displays, choose **No** to configure the new server as a subsequent node.	See Step 10 in the "Performing the Basic Installation" section on page 30.
Step 6	Follow the procedure to configure a subsequent node in the cluster.	See the "Configuring a Subsequent Node" section on page 32.
Step 7	Perform all post-installation tasks that apply to your site.	For a list of post-installation tasks, see Table 13.

Add a New Node to an Existing Cluster

To add a new node to an existing cluster, follow the steps in Table 1.

Table 6 Adding a New Node to an Existing Cluster

	Task	For More Information
Step 1	Before you make any changes to your existing cluster, be sure that you have a current backup file.	For more information, refer to the *Disaster Recovery System Administration Guide*.
Step 2	Perform all pre-installation tasks that apply to your site.	For a list of pre-installation tasks, see Table 1.
Step 3	Ensure that you have the appropriate number of licenses to support adding a new node.	For more information on specifying the required number of licenses, refer to the License Unit Calculator chapter in the *Cisco Unified Communications Manager Administration Guide*.
Step 4	Before you install the new node, ensure that you have configured it on the first node.	From Cisco Unified Communications Manager Administration on the first node, choose **System > Server** and configure the IP address for the subsequent nodes. For more information, see the *Cisco Unified Communications Manager Administration Guide*.
Step 5	Record the configuration settings for each server that you plan to install.	To record your configuration settings, see Table 10 on page 14.
Step 6	You must install the same software version on all nodes in the cluster. If you do not have the correct version on DVD, you need to download updated software from Cisco.com.	
Step 7	Follow the procedure to begin installing the software from the DVD to your server.	See "Starting the Installation" section on page 23.
Step 8	Follow the procedure for performing the basic installation.	See "Performing the Basic Installation" section on page 30.
Step 9	When the First Node Configuration displays, choose **No** to configure the new server as a subsequent node.	See Step 10 in the "Performing the Basic Installation" section on page 30.
Step 10	Follow the procedure for configuring a subsequent node.	See the "Configuring a Subsequent Node" section on page 32.
Step 11	Perform all post-installation tasks that apply to your site.	See Table 13 on page 34.
Step 12	If your cluster is running in mixed mode, ensure that you have your USB key and the latest CTL Client installed on the PC that you use to communicate with the first node. After you finish installing the new node, you will need to update the CTL file on all nodes.	For more information, see "Applying Security to a New Node in a Secure Cluster" section on page 36.

Reusing the MCS-7828 After Installing Cisco Unified Communications Manager Business Edition 5000

If you have installed Cisco Unified Communications Manager Business Edition 5000 on an MCS-7828 server, and you decide that you need to migrate to separate Cisco Unified Communications Manager and Cisco Unity Connection environments for increased scalability and capacity, you can reuse that MCS-7828 server to run Cisco Unified Communications Manager in a MCS-7825 cluster. Although you can reuse the server, you must reenter your data on the server manually. You must also obtain another server to run Cisco Unity Connection.

Note You cannot install Cisco Unified Communications Manager on an MCS-7828 server unless you have previously installed Cisco Unified Communications Manager Business Edition 5000.

To migrate from Cisco Unified Communications Manager Business Edition 5000 to separate Cisco Unified Communications Manager and Cisco Unity Connection environments, follow the steps in Table 7:

Table 7 Reusing the MCS-7828 After Installing Cisco Unified Communications Manager Business Edition 5000

	Task	For More Information
Step 1	Order a single migration SKU (CUCM-BE-MIG). The migration SKU ships with software install media that is required to install Cisco Unified Communications Manager and Cisco Unity Connection. The SKU provides a node license for the Cisco Unified Communications Manager and enables you to migrate the DLUs to Cisco Unified Communications Manager.	For ordering information, refer to the *Cisco Unified Communications Solutions Ordering Guide*. To access the guide, go to www.cisco.com/go/unified-techinfo, choose the appropriate solution release version, choose the Resource Library tab, choose the Ordering Guides link, and choose *Ordering Guide Cisco Unified Communications Management Solutions.*
Step 2	Rehost all device licenses in the Cisco Unified Communications Manager environment by sending a request to licensing@cisco.com. You must include the MAC address and proof of purchase of your devices.	
Step 3	Obtain a new server for Cisco Unity Connection.	
Step 4	Rehost all voice-messaging and advanced user licenses by sending an email to licensing@cisco.com. You must include the MAC address and proof of purchase of the server on which you plan to install Cisco Unity Connection.	
Step 5	Install Cisco Unified Communications Manager on the MCS-7828 server.	Make sure to read this document and the related release notes before beginning the installation.
Step 6	Install Cisco Unity Connection on a new server.	Refer to the *Installation Guide for Unity Connection* that is located at the following URL: http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html.

Parallel Installations of Cluster Nodes

When you install a cluster, you can begin the installation of the first node and subsequent nodes at the same time. When the installation program prompts you to designate the first node as the first node, stop installing on the subsequent nodes until the installation completes on the first node. Then configure the subsequent node(s) on the first node. You can then continue the installation on the subsequent nodes. For optimal performance, you should choose the **Skip** option rather than the **Proceed** option in the installation program.

Pre-Installation Tasks

Table 1 contains a list of pre-installation tasks that you need to perform to ensure that you can successfully install Cisco Unified Communications Manager.

Table 8 Pre-Installation Tasks

	Task	Important Notes
Step 1	Read this entire document to familiarize yourself with the installation procedure.	
Step 2	Verify the integrity of any new server hardware (such as hard drives and memory) by running any manufacturer-provided utilities.	
Step 3	Ensure that your servers are listed as supported hardware and sized appropriately to support the load of the cluster.	For information about the capacity of server models, refer to the documentation at the following URL: http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html Make sure to account for any growth that has occurred since initial system configuration.
Step 4	If you are installing a cluster or adding a node, verify that the links between servers meet the 80-ms round-trip time (RTT) requirement and that you have enough bandwidth to support database replication.	For more information on the 80-ms RTT requirement, refer to the *Cisco Unified Communications Solution Reference Network Design (SRND) Based on Cisco Unified Communications Manager,* which you can find at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html
Step 5	If you are getting the system time from an NTP server, verify that the first node can synchronize with the NTP server before you install a subsequent node. To verify the NTP status of the first node, log into the Command Line Interface on the first node and enter the following command: **utils ntp status** **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are usingIPv6 addressing, external NTP servers must be NTP v4.	For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*. ⚠ **Caution** If the first node fails to synchronize with an NTP server, installation of a subsequent node can also fail.
Step 6	If your firewall is not in the routing path, disable the firewall between nodes, if possible. Also, increase the firewall timeout settings until after you complete the installation.	To temporarily allow network traffic in and out of the nodes (for example, setting the firewall rule for these nodes to `IP any/any`) does not always suffice. The firewall might still close necessary network sessions between nodes due to timeouts.
Step 7	Do not run Network Address Translation (NAT) or Port Address Translation (PAT) between Cisco Unified Communications Manager nodes.	

Table 8 Pre-Installation Tasks (continued)

	Task	Important Notes
Step 8	Record the network interface card (NIC) speed and duplex settings of the switch port to which you will connect the new server. You should configure the same NIC settings on the server and on the switch port. For GigE (1000/FULL), you should set NIC and switch port settings to Auto/Auto; do not set hard values.	Enable PortFast on all switch ports that are connected to Cisco servers. With Portfast enabled, the switch immediately brings a port from the blocking state into the forwarding state by eliminating the forwarding delay [the amount of time that a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state].
Step 9	If you use DNS, verify that all servers on which you plan to install Cisco Unified Communications Manager are properly registered in DNS.	For more information, see the "Verifying DNS Registration" section on page 13.
Step 10	Obtain a Cisco Unified Communications Manager license file.	See "Obtaining a License File" section on page 20. **Note** For more information on specifying the required number of licenses, refer to the License Unit Calculator chapter in the *Cisco Unified Communications Manager Administration Guide*.
Step 11	Record the configurations settings for each server that you plan to install.	To record your configuration settings, see Table 10.
Step 12	Configure any subsequent nodes on the first node before you install a subsequent node.	From Cisco Unified Communications Manager Administration on the first node, choose **System > Server** and configure the IP address for the subsequent nodes. For more information, see the *Cisco Unified Communications Manager Administration Guide.*

Important Considerations

Before you proceed with the installation, consider the following requirements and recommendations:

- Be aware that when you install on an existing server, the hard drive gets formatted, and all existing data on the drive gets overwritten.
- Do not install Cisco Unified Communications Manager in a large Class A or Class B subnet that contains a large number of devices.

  When you install Cisco Unified Communications Manager in a large subnet with a large number devices in that subnet, the Address Resolution Protocol (ARP) table can fill up quickly (maximum 1024 entries, by default). When the ARP table gets full, Cisco Unified Communications Manager can have difficulty talking to endpoints and cannot add more phones.
- Ensure that you connect each Cisco Unified Communications Manager node to an uninterruptible power supply (UPS) to provide backup power and protect your system. Failure to do so may result in damage to physical media and require a new installation of Cisco Unified Communications Manager.

Note You must connect MCS-7816 and MCS-7825 servers to a UPS in order to prevent file system corruption during power outages.

If you want the Cisco Unified Communications Manager node to automatically monitor UPS signaling and automatically initiate a graceful shutdown upon power loss, you should use specific UPS and server models. For more information on supported models and configurations, refer to the *Release Notes for Cisco Unified Communications Manager*.

- Install the Cisco Unified Communications Manager software on the first node first and then on the subsequent nodes.
- Make sure that the subsequent node servers that you are installing can connect to the first node server during the installation.
- When you enter the Security password on the first node, be sure that you write it down and save it. You must enter the same password on each subsequent node that you install in the cluster. Install the software during off-peak hours or a maintenance window to avoid impact from interruptions.
- All servers in a cluster must run the same release of Cisco Unified Communications Manager. The only exception is during a cluster software upgrade, during which a temporary mismatch is allowed.
- Configure the server by using static IP addressing to ensure that the server obtains a fixed IP address and that the Cisco Unified IP Phones can register with the application when you plug the phones into the network.
- Do not attempt to perform any configuration tasks during the installation.
- Do not install any Cisco-verified applications until you complete the installation.
- Be aware that directory names and filenames that you enter while you are running the installation program are case-sensitive.
- Disk mirroring on server model 7825 I3 with 160 GB SATA disk drives takes approximately 3 hours.
- Disk mirroring on server model 7828 I3 with 250 GB SATA disk drives takes approximately 4 hours.
- For a short period of time after you install Cisco Unified Communications Manager or switch over after upgrading to a different product version, settings changes made by phone users might get unset. Examples of phone user settings include call forwarding and message waiting indication light settings. This can occur because Cisco Unified Communications Manager synchronizes the database after an installation or upgrade, which can overwrite phone user settings changes.
- You will face a problem during RAID creation when you install Cisco Unified Communications Manager 8.5 or an earlier version on 7825 H3 and 7528 H3 servers that currently have Cisco Unified Communications Manager 8.6 installed on it. To resolve the issue:
  - **a.** Boot the Cisco Unified CM server with the Cisco Unified CM 8.6 recovery disc.
  - **b.** When prompted, choose option **C** to wipe off all data from the system. Option C indicates “Cleaning the system to set to bare metal state.”

  You can now proceed with the installation of the earlier versions of Cisco Unified CM.
- When you insert or remove a USB drive, you might see error messages on the console similar to “sdb: assuming drive cache: write through.” You can safely ignore these messages.
- Carefully read the information that follows before you proceed with the installation.

Frequently Asked Questions About the Installation

The following section contains information about commonly asked questions and responses. Review this section carefully before you begin the installation.

What User Names and Passwords Do I Need to Specify?

Note The system checks your passwords for strength. For guidelines on creating a strong passwords, see the "What is a Strong Password?" section on page 12.

During the installation, you must specify the following user names and passwords:

- Administrator Account user name and password
- Application User name and password
- Security password

Administrator Account User Name and Password

You use the Administrator Account user name and password to log in to the following areas:

- Cisco Unified Communications Operating System Administration
- Disaster Recovery System
- Command Line Interface

To specify the Administrator Account user name and password, follow these guidelines:

- Administrator Account user name—The Administrator Account user name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Administrator Account password—The Administrator Account password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Administrator Account password or add a new Administrator account by using the command line interface. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Application User Name and Password

You use the Application User name and password to access applications that are installed on the system, including the following areas:

- Cisco Unified Communications Manager Administration
- Cisco Unified Serviceability
- Real Time Monitoring Tool
- Cisco Unified Reporting

To specify the Application User name and password, follow these guidelines:

- Application User name—The Application User name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Application User password—The Application User password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

You can change the Application User name and password by using the command line interface. For more information, see the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Security Password

The system uses this password to authorize communications between nodes, and you must ensure that this password is identical on all nodes in the cluster.

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores.

What is a Strong Password?

The installation wizard checks to ensure that you enter a strong password. To create a strong password, follow these recommendations:

- Mix uppercase and lowercase letters.
- Mix letters and numbers.
- Include special symbols.
- Remember that longer passwords are stronger and more secure than shorter ones.

Avoid the following types of passwords:

- Do not use recognizable words, such as proper names and dictionary words, even when combined with numbers.
- Do not invert recognizable words.
- Do not use word or number patterns, like aaabbb, qwerty, zyxwvuts, 123321, and so on.
- Do not use recognizable words from other languages.
- Do not use personal information of any kind, including birthdays, postal codes, names of children or pets, and so on.

Which Servers Does Cisco Support for this Installation?

For information about supported server models, refer to the following documentation:

- Release notes for your product release
- http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html.

May I Install Other Software on the Server?

You must do all software installations and upgrades by using Cisco Unified Communications Operating System Administration. The system can upload and process only software that Cisco Systems approved.

You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Cisco Unified Communications Manager with Cisco Unified Communications Manager 8.5(1).

Browser Requirements

You can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Cisco Unified Reporting, Cisco Unified Communications Operating System Administration, and Disaster Recovery System by using the browsers and operating systems listed in Table 9 on page 13. Cisco does not support or test other browsers.

Table 9 Supported Browsers and Operating Systems

You can access Cisco Unified Communications Manager with this browser...	...if you use one of these operating systems
Microsoft Internet Explorer 8	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (with latest service pack available)
Mozilla Firefox 3.x or 4.x (if available)	• Microsoft Windows XP SP3 • Microsoft Windows Vista SP2 (or latest service pack available) • Microsoft Windows 7 (32-bit) (latest service pack available) • Apple MAC OS X (latest service pack available)
Safari 4.x or 5.x (if available)	Apple MAC OS X (or newest OS release available)

Verifying DNS Registration

If you use DNS, verify that all servers to be added are registered in DNS properly by performing the following actions:

Procedure

Step 1 Open a command prompt.

Step 2 To ping each server by its DNS name, enter **ping** *DNS_name*.

Step 3 To look up each server by IP address, enter **nslookup** *IP_address*.

Gathering Information for an Installation

Use Table 10 to record the information about your server. Gather this information for each Cisco Unified Communications Manager server that you are installing in the cluster. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration. You should make copies of this table and record your entries for each server in a separate table, even if you are planning to use the DMABackupInfo.inf file to configure your system.

Note Because some of the fields are optional, they may not apply to your configuration. For example, if you choose not to set up an SMTP host during installation, the parameter still displays, but you do not need to enter a value.

Caution You cannot change some of the fields after installation without reinstalling the software, so be sure to enter the values that you want.

The last column in the table shows whether you can change a field after installation, and if you can, it provides the appropriate Command Line Interface (CLI) command.

Caution If Cisco Unified Communications Manager is running on VMware, changing some of these values after installation will require you to obtain updated licenses.

Table 10 Node Configuration Data

Parameter	Description	Can Entry Be Changed After Installation?
Administrator ID Your entry:	This field specifies the administrator account user ID that you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration and for logging into the Disaster Recovery System.	No, you cannot change the entry after installation. **Note** After installation, you can create additional administrator accounts, but you cannot change the original administrator account user ID.
Administrator Password Your entry:	This field specifies the password for the Administrator account, which you use for secure shell access to the CLI, for logging into Cisco Unified Communications Operating System Administration and for logging into the Disaster Recovery System. Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password admin**

Table 10 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Application User Name Your entry:	You use the Application User name as the default user name for applications that are installed on the system, including Cisco Unified Communications Manager and Cisco Unified Serviceability. ⚠ **Caution**	Yes, you can change the entry after installation by using the following CLI command: CLI > **utils reset_ui_administrator_name**
Application User Password Your entry:	You use the Application User password as the default password for applications that are installed on the system, including Cisco Unified Communications Manager and Cisco Unified Serviceability.	Yes, you can change the entry after installation by using the following CLI command: CLI > **utils reset_ui_administrator_password**
Country Your entry:	From the list, choose the appropriate country for your installation. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
DHCP Your entry:	If you want to use DHCP to automatically configure the network settings on your server, choose **Yes**. If you choose **Yes**, you do not get prompted for DNS or static configuration settings. If you choose **No**, you must enter a hostname, IP Address, IP Mask, and Gateway.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dhcp**
DNS Enable Your entry:	A DNS server resolves a hostname into an IP address or an IP address into a hostname. If you do not have a DNS server, enter **No**. If you have a DNS server, Cisco recommends that you enter **Yes** to enable DNS. **Note** When DNS is not enabled, you should only enter IP addresses (not host names) for all network devices in your Cisco Unified Communications Manager network.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns**

Table 10 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
DNS Primary Your entry:	Enter the IP address of the DNS server that you want to specify as the primary DNS server. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd. Consider this field mandatory if DNS is set to **yes** (DNS enabled).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns** ⚠ **Caution** To avoid potential problems related to ITL for this change, refer to the “Initial Trust List and Certificate Regeneration” section in *Changing the IP Address and Host Name for Cisco Unified Communications Manager* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
DNS Secondary (optional) Your entry:	Enter the IP address of the DNS server that you want to specify as the optional secondary DNS server.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network dns** ⚠ **Caution** To avoid potential problems related to ITL for this change, refer to the “Initial Trust List and Certificate Regeneration” section in *Changing the IP Address and Host Name for Cisco Unified Communications Manager* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
Domain Your entry:	This field represents the name of the domain in which this machine is located. Consider this field mandatory if DNS is set to **yes**.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network domain** ⚠ **Caution** To avoid potential problems related to ITL for this change, refer to the “Initial Trust List and Certificate Regeneration” section in *Changing the IP Address and Host Name for Cisco Unified Communications Manager* at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

Table 10 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Gateway Address Your entry:	Enter the IP address of the network gateway. If you do not have a gateway, you must still set this field to 255.255.255.255. Not having a gateway may limit you to only being able to communicate with devices on your subnet. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network gateway**
Hostname Your entry:	Enter a host name that is unique to your server. The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens. The first character cannot be a hyphen. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the entry after installation. For information, refer to the document *Changing the IP Address and Host Name for Cisco Unified Communications Manager* for your product release at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
IP Address Your entry:	Enter the IP address of your server. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the entry after installation. For information, refer to the *Changing the IP Address and Host Name for Cisco Unified Communications Manager 5.x, 6.x, and 7.x Servers* document at the following URL: http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.
IP Mask Your entry:	Enter the IP subnet mask of this machine. If DHCP is set to **No**, consider this field mandatory.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network ip eth0**
Location Your entry:	Enter the location of the server. The system uses this information to generate certificate signing requests (CSRs), which are used to obtain third-party certificates. You can enter any location that is meaningful within your organization. Examples include the state or the city where the server is located.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Table 10 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
MTU Size Your entry:	The maximum transmission unit (MTU) represents the largest packet, in bytes, that this host will transmit on the network. Enter the MTU size in bytes for your network. The MTU size that you configure must not exceed the lowest MTU size that is configured on any link in your network. Default: 1500 bytes The MTU setting must be the same on all nodes in a cluster.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network mtu**
NIC Duplex Your entry:	Choose the duplex mode for the network interface card (NIC), either Full or Half. **Note** This parameter only displays when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**
NIC Speed Your entry:	Choose the speed for the NIC, either 10 megabits per second or 100 megabits per second. **Note** This parameter only displays when you choose not to use Automatic Negotiation.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set network nic**
NTP Server Your entry:	Enter the hostname or IP address of one or more network time protocol (NTP) servers with which you want to synchronize. You can enter up to five NTP servers. **Note** To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4). If you are usingIPv6 addressing, external NTP servers must be NTP v4. **Note**	Yes, you can change the entry after installation by using the Cisco Unified Communications Operating System: **Settings > NTP Servers**

Table 10 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Organization Your entry:	Enter the name of your organization. **Tip** You can use this field to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**
Security Password Your entry:	Servers in the cluster use the security password to communicate with one another. The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character. **Note** Save this password. You will be asked to enter the same security password for each subsequent node in the cluster.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set password security** **Caution** To avoid losing communications between nodes, you must change the Security password on all nodes in a cluster and reboot all of the nodes. For more information, refer to the description of this command in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.
SMTP Location Your entry:	Enter the hostname or IP address for the SMTP server that is used for outbound e-mail. The hostname can contain alphanumeric characters, hyphens, or periods, but it must start with an alphanumeric character. **Note** You must fill in this field if you plan to use electronic notification.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set smtp**
State Your entry:	Enter the state where the server is located. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Table 10 Node Configuration Data (continued)

Parameter	Description	Can Entry Be Changed After Installation?
Time Zone Your entry:	This field specifies the local time zone and offset from Greenwich Mean Time (GMT). Choose the time zone that most closely matches the location of your machine.	Yes, you can change the entry after installation by using the following CLI command: CLI > **set timezone**
Unit Your entry:	Enter your unit. **Note** The value you enter gets used to generate a Certificate Signing Request (CSR).	Yes, you can change the entry after installation by using the following CLI command: CLI > **set web-security**

Obtaining a License File

Licensing helps manage Cisco Unified Communications Manager licenses and enforces the licenses for Cisco Unified Communications Manager applications and the number of IP phones. This section provides information on obtaining licenses for new Cisco Unified Communications Manager systems and/or phone installations as well as for Cisco Unified Communications Manager nodes that have been upgraded from various releases.

Though Cisco Unified Communications Manager is now priced and ordered via user licenses called User Connect Licenses (UCL) or Cisco Unified Workspace Licenses (CUWL), the Cisco Unified Communications Manager still uses Device License Units (DLU), server node licenses and SW Feature Licenses. The appropriate conversion in licensing is made at time of order and delivered via the Product Authorization Key (PAK) as explained in the following section.

New Cisco Unified Communications Manager Servers and Devices

Use the following procedure to obtain a node license file for new Cisco Unified Communications Manager servers and to obtain device licenses for new devices that require additional device license units.

Each node in your cluster requires one node license unit. Each device type requires a fixed number of licenses units, depending on the type. For example, Cisco Unified IP Phone 7920 require four license units, and Cisco Unified IP Phone 7970 require five units. If you want licenses for four Cisco Unified IP Phones 7920 and four Cisco Unified IP Phones 7970 phones, you require 36 phone license units.

You use the Product Authorization Key (PAK) that came with your product to obtain the necessary permanent licenses, as described in the following procedure.

Procedure

Step 1 Enter the Product Authorization Key (PAK) that you received with your Cisco Unified Communications Manager or phone order in the License Registration web tool at http://www.cisco.com/go/license.

Step 2 Click **Submit**.

Step 3 Follow the system prompts. You must enter the MAC address of the Ethernet 0 NIC of the first node of the Cisco Unified Communications Manager cluster. You must enter a valid e-mail address as well as the number of nodes and device license units for which you want licenses.

Note For information on calculating the number of device license units that are required for the devices in your system, refer to the "License Unit Calculator" section in the *Cisco Unified Communications Manager Administration Guide*.

The system sends the license file(s) to you via e-mail by using the E-mail ID that you provided. The format of a license file 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.

Note One license file may apply to more than one node in your cluster. For information on how to interpret the license file, see the "License File Contents" section of the *Cisco Unified Communications Manager System Guide*.

Step 4 You must upload the license file to the server with the matching MAC address that you provided in Step 3. See the "Uploading a License File" section on page 35. This server then takes on the functionality of the license manager.

You can use the licenses that are specified in the license file only within the cluster on which the license file is uploaded.

Using the Cisco Unified Communications Answer File Generator

Cisco Unified Communications Answer File Generator, a web application, generates answer files for unattended installations of Cisco Unified Communications Manager. Individual answer files get copied to the root directory of a USB key or a floppy diskette and are used in addition to the Cisco Unified Communications Manager DVD during the installation process.

The web application supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installs on the publisher server and all subscriber servers.
- Provides syntactical validation of data entries.
- Provides online help and documentation.

The following usage requirements apply:

- The web application supports only fresh installs and does not support upgrades.
- If DHCP client is being used on the publisher server, and subscriber server answer files are also being generated, you must specify the publisher server IP address.

You can access the Cisco Unified Communications Answer File Generator at the following URL:

http://www.cisco.com/web/cuc_afg/index.html

The Cisco Unified Communications Answer File Generator supports Internet Explorer version 6.0 or higher and Mozilla version 1.5 or higher.

Note Cisco requires that you use USB keys that are compatible with Linux 2.4. Cisco recommends that you use USB keys that are preformatted to be compatible with Linux 2.4 for the configuration file. These keys will have a W95 FAT32 format.

Handling Network Errors During Installation

During the installation process, the installation program verifies that the server can successfully connect to the network by using the network configuration that you enter. If it cannot connect, a message displays, and you get prompted to select one of the following options:

- **RETRY** —The installation program tries to validate networking again. If validation fails again, the error dialog box displays again.
- **REVIEW (Check Install)**—This option allows you to review and modify the networking configuration. When detected, the installation program returns to the network configuration windows.

  Networking gets validated after you complete each networking window, so the message might display multiple times.
- **HALT**— The installation halts. You can copy the installation log files to a USB disk to aid troubleshooting of your network configuration.
- **IGNORE** —The installation continues. The networking error gets logged. In some cases, the installation program validates networking multiple times, so this error dialog box might display multiple times. If you choose to ignore network errors, the installation may fail.

Installation Overview

The installation process allows you to perform a basic installation or upgrade to a newer service release during the installation.

For a more detailed description of the different installation types, see Table 11.

Table 11 Installation Options

Installation Types	Description
Basic Install	This option represents the basic Cisco Unified Communications Manager 8.6(1) installation, which installs the software from the installation disc and does not use any imported data.
Applying a Patch (upgrade during install)	This option allows you to upgrade the software version that is contained on the installation disc with a later release. You can only apply one patch during the installation process. **Note** Ensure that you have the software image available on DVD or on a remote server prior to choosing this option.

Installing the New Operating System and Application

This section describes how to install the operating system and Cisco Unified Communications Manager application. You install the operating system and application by running one installation program. This document divides the procedure for using this installation program into the following major topics:

- Navigating Within the Installation Wizard, page 23
- Starting the Installation, page 23
- Entering Preexisting Configuration Information, page 25
- Performing the Basic Installation, page 30
- Configuring the First Node, page 31
- Configuring a Subsequent Node, page 32

Navigating Within the Installation Wizard

For instructions on how to navigate within the installation wizard, see Table 12.

Table 12 Installation Wizard Navigation

To Do This	Press This
Move to the next field	**Tab**
Move to the previous field	**Alt-Tab**
Choose an option	Space bar or **Enter**
Scroll up or down in a list	Up or down arrow
Go to the previous window	Space bar or **Enter** to choose **Back** (when available)
Get help information on a window	Space bar or **Enter** to choose **Help** (when available)

Starting the Installation

To start the installation, follow this procedure.

Note If you are installing a subsequent node or adding a node to an existing cluster, you must configure the host name or IP address of the new node on the first node in the cluster. From Cisco Unified Communications Manager Administration on the first node, choose **System > Server** and enter the IP address or host name of the subsequent node. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 If you have a USB key with configuration information that the Answer File Generator generated, insert it now.

Note If you have a new server with the software preinstalled, you do not need to install from a DVD, unless you want to reimage the server with a later product release. You can go directly to the "Entering Preexisting Configuration Information" procedure on page 25.

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 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 Media Check Result window displays. 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 from Cisco.com or obtain another DVD directly from Cisco.

Step 5 The system installer performs the following hardware checks to ensure that your system is correctly configured. If the installer makes any changes to your hardware configuration settings, you will get prompted to restart your system. Leave the DVD in the drive during the reboot:

- First, the installation process checks for the correct drivers, and you may see the following warning:

```
No hard drives have been found. You probably need to manually choose device drivers
for install to succeed. Would you like to select drivers now?
```

  To continue the installation, choose **Yes**.

- The installation next checks to see whether you have a supported hardware platform. If your server does not meet the exact hardware requirements, the installation process fails with a critical error. If you think this is not correct, capture the error and report it Cisco support.
- The installation process next verifies RAID configuration and BIOS settings.

Note For MCS 7825 H3 and MCS 7828 H3 Server models, the installation process detects and disables the SATA RAID, if enabled. The "System Rebooting Intermediately" window appears with the message `System is going to reboot for SATA RAID to be disabled in BIOS Press any key to continue`. This disables the SATA RAID and reboots the system. On reboot, the installation will continue and will activate the Linux SW RAID.

Note If this step repeats, choose **Yes** again.

- If the installation program must install a BIOS update, a notification appears telling you that the system must reboot. Press any key to continue with the installation.

After the hardware checks complete, the Product Deployment Selection window displays.

Step 6 In the Product Deployment Selection window, select the product to install; then, choose **OK**. You can choose from the following options:

- Cisco Unified Communications Manager
- Cisco Unity Connection

- Cisco Unified Communications Manager Business Edition 5000 (includes Cisco Unified Communications Manager and Cisco Unity Connection)

Note The window indicates which products are supported and not supported by your hardware. If only one product is supported, you do not choose which product to install.

Step 7 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.

The Platform Installation Wizard window displays.

Step 8 Choose one of the following options:

- To enter your configuration information manually and have the installation program install the configured software on the server, choose **Proceed** and continue with this procedure.
- To do any of the following tasks, choose **Skip** and continue with the "Entering Preexisting Configuration Information" procedure on page 25:
  - Manually configure the software that is preinstalled on your server—In this case you do not need to install the software, but you must configure the preinstalled software.
  - Perform an unattended installation—In this case, you provide preexisting configuration information on a USB key or floppy disk.
  - Install the software before manually configuring it—In this case the installation program installs the software, then prompts you to configure it manually. You can choose **Skip** if you want to preinstall the application on all your servers first and then enter the configuration information at a later time. This method might cause you to spend more time performing the installation than the other methods.

Step 9 Choose the type of installation to perform by doing the following steps. See Table 11 for more information on installation options.

In the Apply Additional Release window, choose one of the options:

- To upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the "Applying a Patch" section on page 26.
- To skip this step, choose **No**.
- To return to the previous window, choose **Back**.

Step 10 In the Basic Install window, choose **Continue** to install the software version on the DVD or configure the preinstalled software. Continue with the "Performing the Basic Installation" section on page 30.

Entering Preexisting Configuration Information

Start here if you have a server that has the product preinstalled or if you chose **Skip** in the Platform Installation Wizard window.

Procedure

Step 1 After the system restarts, the Preexisting Installation Configuration window displays.

Step 2 If you have preexisting configuration information that the Answer File Generator created, that is stored on a floppy disc or a USB key, insert the disc or the USB key now and choose **Continue**. The installation wizard will read the configuration information during the installation process.

Note If a popup window states that the system detected new hardware, press any key and then choose **Install** from the next window.

The Platform Installation Wizard window displays.

Step 3 To continue with the Platform Installation Wizard, choose **Proceed**.

Step 4 Choose the type of installation to perform by doing the following steps. See Table 11 for more information on installation options.

In the Apply Additional Release window, choose one of the options:

- To upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the “Applying a Patch” section on page 26.
- To skip this step, choose **No**.
- To return to the previous window, choose **Back**.

Step 5 In the Basic Install window, choose **Continue**. Continue with the “Performing the Basic Installation” section on page 30.

Applying a Patch

If you choose **Yes** in the Apply a Patch window, the installation wizard installs the software version on the DVD first and then restarts the system. You must obtain the appropriate upgrade file from Cisco.com before you can upgrade during installation.

Note You can upgrade to any supported higher release, so long as you have a full patch, not an ES or an SR, in which case you can only upgrade to a later service release within the same maintenance release.

For information about supported upgrades, see the Release Notes for your product release and the Cisco Unified Communications Manager Compatibility Matrix at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_device_support_tables_list.html

You can access the upgrade file during the installation process from either a local disk (DVD) or from a remote FTP or SFTP server.

Procedure

Step 1 The Install Upgrade Retrieval Mechanism Configuration window displays.

Step 2 Choose the upgrade retrieval mechanism to use to retrieve the upgrade file:

- **SFTP**—Retrieves the upgrade file from a remote server by using the Secure File Transfer Protocol (SFTP). Skip to the "Upgrading from a Remote Server" section on page 27.
- **FTP**—Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the "Upgrading from a Remote Server" section on page 27.
- **LOCAL**—Retrieves the upgrade file from a local DVD. Continue with the "Upgrading from a Local Disk" section on page 27.

Upgrading from a Local Disk

Before you can upgrade from a local disk, you must download the appropriate patch file from Cisco.com and use it to create an upgrade DVD. You must create an ISO image on the DVD from the upgrade file. Just copying the ISO file to a DVD will not work.

Procedure

Step 1 When the Local Patch Configuration window displays, enter the patch directory and patch name, if required, and choose **OK**.

The Install Upgrade Patch Selection Validation window displays.

Step 2 The window displays the patch file that is available on the DVD. To update the system with this patch, choose **Continue**.

Step 3 Choose the upgrade patch to install. The system installs the patch, then restarts the system with the upgraded software version running.

After the system restarts, the Preexisting Configuration Information window displays.

Step 4 To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays.

Step 5 To continue the installation, choose **Proceed** or choose **Cancel** to stop the installation.

If you choose **Proceed**, the Apply Patch window displays. Continue with Step 6.

If you choose **Cancel**, the system halts, and you can safely power down the server.

Step 6 When the Apply Patch window displays, choose **No**.

Step 7 The Windows Upgrade window displays.

Step 8 Choose **No** and continue with the "Performing the Basic Installation" section on page 30.

Upgrading from a Remote Server

Before you can upgrade from a remote server, you must download the appropriate patch file from Cisco.com to an FTP or SFTP server that the server can access.

If you are upgrading from release 5.1(3), you must download the appropriate patch file from Cisco.com, create an ISO image DVD from the patch file, then copy the contents of the DVD to a remote FTP or SFTP server that the server can access.

Cisco allows you to use any SFTP server product but recommends SFTP products that have been certified with Cisco through the Cisco Technology Developer Partner program (CTDP). CTDP partners, such as GlobalSCAPE, certify their products with specified version of Cisco Unified Communications Manager. For information on which vendors have certified their products with your version of Cisco Unified Communications Manager, refer to http://developer.cisco.com/web/cdc/home. For information on using GlobalSCAPE with supported Cisco Unified Communications versions, refer to http://www.globalscape.com/gsftps/cisco.aspx.Cisco uses the following servers for internal testing. You may use one of the servers, but you must contact the vendor for support:

- Open SSH (for Unix systems. Refer to http://sshwindows.sourceforge.net/)
- Cygwin (http://www.cygwin.com/)
- Titan (http://www.titanftp.com/)

Note For issues with third-party products that have not been certified through the CTDP process, contact the third-party vendor for support.

If you chose to upgrade through an FTP or SFTP connection to a remote server, you must first configure network settings so that the server can connect to the network.

Procedure

Step 1 The Auto Negotiation Configuration window displays.

Step 2 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.

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

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

  The MTU Configuration window displays. Continue with Step 4.

- To disable automatic negotiation, choose **No**. The NIC Speed and Duplex Configuration window displays. Continue with Step 3.

Step 3 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 4 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.

Caution If you configure the MTU size incorrectly, your network performance can be affected.

- 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 5 For network configuration, you can choose to either set up static network IP addresses for the node and gateway or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended. If you use DHCP, use static DHCP.

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The installation process attempts to verify network connectivity. Skip to Step 8.
- If you want to configure static IP addresses for the node, choose **No**. The Static Network Configuration window displays.

Step 6 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 10 for field descriptions.

The DNS Client Configuration window displays.

Step 7 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 10 for field descriptions.

After the system configures the network and checks for connectivity, the Remote Patch Configuration window displays.

Step 8 Enter the location and login information for the remote file server. The system connects to the remote server and retrieves a list of available upgrade patches.

If the upgrade file is located on a Linux or Unix server, you must enter a forward slash at the beginning of the directory path. For example, if the upgrade file is in the patches directory, you must enter `/patches`

If the upgrade file is located on a Windows server, remember that you are connecting to an FTP or SFTP server, so use the appropriate syntax, including:

- Begin the path with a forward slash (/) and use forward slashes throughout the path.
- The path must start from the FTP or SFTP root directory on the server, so you cannot enter a Windows absolute path, which starts with a drive letter (for example, C:).

The Install Upgrade Patch Selection window displays.

Step 9 Choose the upgrade patch to install. The system downloads, unpacks, and installs the patch and then restarts the system with the upgraded software version running.

After the system restarts, the Preexisting Configuration Information window displays.

Step 10 To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays.

Step 11 To continue the installation, choose **Proceed** or choose **Cancel** to stop the installation.

If you choose **Proceed**, the Apply Patch window displays. Continue with Step 12.

If you choose **Cancel**, the system halts, and you can safely power down the server.

Step 12 When the Apply Patch window displays, choose **No**.

Step 13 The Windows Upgrade window displays.

Step 14 Choose **No** and continue with the "Performing the Basic Installation" section on page 30.

Performing the Basic Installation

Procedure

Step 1 When the Timezone Configuration displays, choose the appropriate time zone for the server and then choose **OK**.

The Auto Negotiation Configuration window displays.

Step 2 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** and continue with Step 5.

  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 Step 3.

  The NIC Speed and Duplex Configuration window displays.

Step 3 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 4 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 If you configure the MTU size incorrectly, your network performance can be affected.

- 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 5 For network configuration, you can choose to either set up a static network IP address for the node or to use Dynamic Host Configuration Protocol (DHCP). Static IP addresses are recommended. If you use DHCP, use static DHCP

- If you have a DHCP server that is configured in your network and want to use DHCP, choose **Yes**. The network restarts, and the Administrator Login Configuration window displays. Skip to Step 8.
- If you want to configure a static IP address for the node, choose **No**. The Static Network Configuration window displays.

Step 6 If you chose not to use DHCP, enter your static network configuration values and choose **OK**. See Table 10 for field descriptions.

The DNS Client Configuration window displays.

Step 7 To enable DNS, choose **Yes**, enter your DNS client information, and choose **OK**. See Table 10 for field descriptions.

The network restarts by using the new configuration information, and the Administrator Login Configuration window displays.

Step 8 Enter your Administrator login and password from Table 10.

Note The Administrator login must start with an alphabetic character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. You will need the Administrator login to log in to Cisco Unified Communications Operating System Administration, the command line interface, and the Disaster Recovery System.

The Certificate Information window displays.

Step 9 Enter your certificate signing request information and choose **OK**.

The First Node Configuration window displays.

Step 10 You can configure this server as either the first node in a Cisco Unified Communications Manager cluster or as a subsequent node.

- To configure this server as the first Cisco Unified Communications Manager node, choose **Yes** and continue with the "Configuring the First Node" section on page 31.
- To configure this server as a subsequent node in the cluster, choose **No** and continue with the "Configuring a Subsequent Node" section on page 32.

Configuring the First Node

After you finish the basic installation, follow this procedure to configure the server as the first node in the cluster.

Procedure

Step 1 The Network Time Protocol Client Configuration window displays.

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 stratums 1-9). Subsequent nodes in the cluster will get their time from the first node.When you are installing Cisco Unity Connection on a virtual machine, you must specify an external NTP server.

Step 2 Choose whether you want to configure an external NTP server or manually configure the system time.

- 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 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 3 Enter the Security password from Table 10.

Note The Security password must start with an alphanumeric character, be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. The system uses this password to authorize communications between nodes, and you must ensure this password is identical on all nodes in the cluster.

The SMTP Host Configuration window displays.

Step 4 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 platform GUI or the command line interface.

Step 5 Choose **OK**. The Application User Configuration window displays.

Step 6 Enter the Application User name and password from Table 10 and confirm the password by entering it again.

Step 7 Choose **OK**. The Platform Configuration Confirmation window displays.

Step 8 To continue with the installation, choose **OK**; or to modify the platform configuration, choose **Back**.

The system installs and configures the software. The DVD drive ejects, and the server reboots. Do not reinsert the DVD.

Step 9 When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 10 Complete the post-installation tasks that are listed in the "Post-Installation Tasks" section on page 33.

Configuring a Subsequent Node

To configure a subsequent node in the cluster, follow these steps.

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 *Cisco Unified Communications Manager Administration Guide*.

Procedure

Step 1 If you configured Network Time Protocol on the first node, ensure that it is synchronized with an NTP server before you install a subsequent node. From the Command Line Interface on the first node, enter **utils ntp status**. Ensure that the output 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 On the First Node Configuration window, read the Warning and make sure you have correctly configured the first node. To continue with the installation of the subsequent node, click **OK**.

The Network Connectivity Test Configuration window displays.

Step 3 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 4 Enter the first node connectivity information and choose **OK**.

The system checks for network connectivity.

If you chose to pause the system after the system successfully verifies 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 5 If you want to configure an SMTP server, choose **Yes** and enter the SMTP server name.

Note To use certain operating system features, you must configure an SMTP server; 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 6 To start installing the software, choose **OK**, or, if you want to change the configuration, choose **Back**.

Step 7 When the installation process completes, you get prompted to log in by using the Administrator account and password.

Step 8 Complete the post-installation tasks that are listed in the "Post-Installation Tasks" section on page 33.

Post-Installation Tasks

After installing Cisco Unified Communications Manager on your server, you must set some configuration parameters and perform other post-installation tasks before you can begin using it. Perform these tasks for the server that you install and complete the tasks before other servers in the cluster are installed.

For post-installation tasks that you must complete after the installation, see Table 13.

Table 13 Post-Installation Tasks

Post-Installation Tasks	Important Notes
Log in as the Cisco Unified Communications Manager Application User and change the Application User passwords.	See the "Changing the Default Application User Passwords" section on page 35.
Install Real Time Monitoring Tool.	You can use Real Time Monitoring Tool to monitor system health, and view and collect logs. For installation instructions and more information about Real Time Monitoring Tool, see the *Cisco Unified Real Time Monitoring Tool Administration Guide*.
Configure the netdump utility, if you installed a cluster of servers.	The netdump utility allows you to send data and memory crash dump logs from one server on the network to another. For instructions for configuring the netdump utility, refer to the *Troubleshooting Guide*
Upload your Cisco Unified Communications Manager license files to the first node.	See the "Uploading a License File" section on page 35.
Activate Cisco Unified Communications Manager feature services that you want to run. Before you activate feature services, you must perform required preactivation tasks. For service activation requirements, refer to the *Cisco Unified Serviceability Administration Guide*.	Refer to *Cisco Unified Serviceability Administration Guide*. See the "Accessing Cisco Unified Serviceability" section on page 35.
Configure the backup settings. Remember to back up your Cisco Unified Communications Manager data daily.	Refer to *Disaster Recovery System Administration Guide*.
The locale English_United_States installs automatically on the server; however, you can add new locales to the server, if required.	Refer to *Cisco Unified Communications Operating System Administration Guide*.
Install COP enabler files for any custom device types that you want to use that do not ship with Cisco Unified Communications Manager.	
If applicable, configure any network management systems in use at your site.	Refer to the *Cisco Unified Serviceability Administration Guide*.
If you want to set up a secure cluster, you can run your Cisco IP Telephony network in mixed mode.	For more information, see the "Installing the CTL Client" and "Configuring the CTL Client" procedures in the *Cisco Unified Communications Manager Security Guide*.
Configure the system.	See the"Configuring the Database" section on page 36. For more information, refer to the *Cisco Unified Communications Manager System Guide*.

Changing the Default Application User Passwords

The installation sets all Application User passwords to the same Application User password that you entered during installation. Cisco recommends that you log in to Cisco Unified Communications Manager Administration and change these passwords. Refer to *Cisco Unified Communications Manager Administration Guide* for the procedure for changing a password.

Accessing Cisco Unified Serviceability

To access Cisco Unified Communications Manager Administration or Cisco Unified Serviceability, you will need to use a web browser from a PC with network access to the Cisco Unified Communications Manager server.

Even though all services are installed on each server in the cluster, you must manually activate the services that you want to run on each server in the cluster through Cisco Unified Serviceability. For service recommendations and more information, refer to *Cisco Unified Serviceability Administration Guide*.

Uploading a 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 "Obtaining a License File" section on page 20. 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 on the first node of the Cisco Unified Communications Manager cluster.

Procedure

Step 1 Choose **System > Licensing > License File Upload**.

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, click **View File**.

Step 3 To choose a new license file to upload, click **Upload License File**.

The Upload File pop-up window displays.

Step 4 To upload to the server, click **Browse** to choose a license file.

Note The following format applies for the license file that you receive: 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**.

After the upload process completes, the Upload Result file displays.

Step 6 Click **Close**.

In the License File Upload window, the status of the uploaded file displays.

Note The license file gets uploaded 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. If the version check fails, an alarm gets generated, and you should get a new license file with the correct version. The system bases the version check only on major releases.

Step 7 Restart the Cisco CallManager service. For information on restarting services, refer to the *Cisco Unified Serviceability Administration Guide*.

Applying Security to a New Node in a Secure Cluster

Use the following procedure to apply security to a new node in a secure cluster after you have successfully added the node. For more information on adding a new node to a cluster, see the "Add a New Node to an Existing Cluster" section on page 5.

Note For more information, refer to the "Configuring the CTL Client" procedure in the *Cisco Unified Communications Manager Security Guide*.

Procedure

Step 1 Activate the Cisco CTL Provider service on the new node.

Step 2 Use an etoken from the existing CTL file and run the CTL client again to get the certificates from all the servers in the cluster, including the new server, into the CTL file. You must be running the Cisco CTL Provider on all servers in the cluster to generate the certificates and update the CTL file.

Step 3 Restart the Cisco TFTP service on all TFTP servers.

Step 4 Restart the Cisco CallManager service on all the nodes.

Step 5 Reset all devices to distribute the new CTL file to the devices.

Configuring the Database

After installing Cisco Unified Communications Manager, you use Cisco Unified Communications Manager Administration to begin configuring the database. The Cisco Unified Communications Manager database contains information and parameters that relate to the system as a whole, to connected devices, and to individual users. The following list describes a few tasks that you must perform in Cisco Unified Communications Manager Administration or Cisco Unified Serviceability:

1. In Cisco Unified Serviceability, activate the services that you want to run on each server in the cluster.

2. Configure system-level settings, such as Cisco Unified Communications Manager Groups.
3. Design and configure your dialing plan.
4. Configure media resources for conferences, music on hold, and so on.
5. Configure systemwide features, Cisco Unified IP Phone services, Cisco Unified Communications Manager Extension Mobility, Cisco Unified Communications Manager Attendant Console, and Cisco Unified Communications Manager Assistant.
6. Install and configure the gateways.
7. Enable computer telephony integration (CTI) application support; then, install and configure the desired CTI applications.
8. Configure the users.
9. Configure and install the phones; then, associate users with the phones.

For more information about configuring the Cisco Unified Communications Manager database, refer to the *Cisco Unified Communications Manager Administration Guide,* the *Cisco Unified Communications Manager System Guide,* or online help in the Cisco Unified Communications Manager application.

Examining Log Files

If you encounter problems with the installation, you may be able to examine the install log files by entering the following commands in Command Line Interface.

To obtain a list of install log files from the command line, enter

```
CLI>file list install *
```

To view the log file from the command line, enter

```
CLI>file view install log_file
```

where *log_file* is the log file name.

You can also view logs by using the Real Time Monitoring Tool. For more information on using and installing the Real Time Monitoring Tool, refer to the*Cisco Unified Real Time Monitoring Tool Administration Guide*.

You can get more information about installation events by viewing or downloading the System History log. Refer to the following for more information:

- "Working with Trace and Log Central" chapter in the *Cisco Unified Real Time Monitoring Tool Administration Guide*
- *Troubleshooting Guide*

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance please contact us by sending email to export@cisco.com.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.