Installing Cisco Unified Communications Manager Business Edition 5000, Release 9.0(1)

First Published: May 08, 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27195-01

CONTENTS

Preface

Purpose

This document describes how to install the Cisco Unified Communications Manager Business Edition 5000 software.

Audience

This Installation Guide is intended for administrators who are responsible for installing Cisco Unified Communications Manager Business Edition 5000 software.

Related documentation

For additional Cisco Unified Communications Manager Business Edition 5000 documentation, see http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html.

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

Obtain support

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.

CHAPTER 1

Installing Cisco Unified Communications Manager Business Edition 5000 Release 9.0(1)

Reuse the MCS-7828

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, perform the following steps.

Procedure

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*.

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 (for MCS server deployments) or License MAC (for VMware deployments) 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 (for MCS server deployments) or License MAC (for VMware deployments) 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*.

Pre-installation tasks

Perform all pre-installation tasks to ensure that you can successfully install the Cisco Unified Communications Manager Business Edition 5000.

Procedure

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. Make sure to account for any growth that has occurred since initial system configuration.
For information about the capacity of server models, see *Cisco <model number> Unified Communications Manager Business Edition Appliance* documents at http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_brochure_list.html.

Step 4 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 5 If you use DNS, verify that all servers on which you plan to install Cisco Unified Communications Managers Business Edition 5000 are properly registered in DNS.

Step 6 Obtain a license file.

Note For more information on specifying the required number of licenses, refer to the *Cisco Unified Communications Manager Administration Guide*.

Step 7 Record the configurations settings for each server that you plan to install.

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.
- Ensure that you connect the server 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.

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*.
- 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.
- You may encounter a problem during RAID creation when you install Cisco Unified Communications Manager 8.6 or an earlier version on 7825 H3 and 7528 H3 servers that currently have Cisco Unified Communications Manager 9.0 installed on it. To resolve the issue:

  1 Boot the Cisco Unified CM server with the Cisco Unified CM 9.0 recovery disc.

2 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.
- 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.
- Carefully read the information that follows before you proceed with the installation.

Frequently asked questions

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

Installation time

The entire installation process, excluding pre- and post-installation tasks, takes 45 to 90 minutes, depending on your server type.

User name and password requirements

Note The system checks your passwords for strength. See topics related to password considerations for guidelines on creating a strong password.

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 Unity Connection 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 Unified Communications Solutions*.

Security password

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

Related Topics

Password considerations, on page 5

Password considerations

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 hyphens and underscores.
- 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.

Server support

For information about Cisco Unified Communications Manager Business Edition 5000 supported server models, refer to the following documentation:

- *Cisco <model number> Unified Communications Manager Business Edition Appliance* at http://www.cisco.com/en/US/products/hw/voiceapp/ps378/products_data_sheets_list.html.

Software restrictions

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 unapproved third-party or Windows-based software applications.

Browser requirements

You can access Cisco Unified Communications Manager Administration, Cisco Unified Serviceability, Cisco Unified Communications Operating System Administration, and Disaster Recovery System by using the browsers and operating systems listed in the following table. Cisco does not support or test other browsers.

Table 1: 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)

You can access Cisco Unified Communications Manager with this browser...	...if you use one of these operating systems
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)

For current browser requirements for accessing Cisco Unity Connection Administration and Cisco Unity Connection Serviceability, see *System Requirements for Cisco Unity Connection in Cisco Unified CMBE Release 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucmbesysreqs.html..

Verify 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.

Installation information

Use the following table to record the information about your server. You may not need to obtain all the information; gather only the information that is pertinent to your system and network configuration.

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.

Table 2: Server 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**
Application User Name Your entry:	You use the Application User name as the default user name for applications that are installed on the system, for example, Cisco Unity Connection Administration and Cisco Unity Connection Serviceability. **Caution** Do not specify unityconnection as the Application User Name or the installation will fail.	Yes, you can change the entry after installation by using the following CLI command: **CLI > utils reset_ui_administrator_name**

Parameter	Description	Can Entry Be Changed After Installation?
Application User Password Your entry:	You use the Application User password as the default password for applications that are installed on the system, for example, Cisco Unity Connection Administration and Cisco Unity Connection 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 network.	Yes, you can change the entry after installation by using the following CLI command: **CLI > set network dns**
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**

Parameter	Description	Can Entry Be Changed After Installation?
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**
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** CLI > set network
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.
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.
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**

Parameter	Description	Can Entry Be Changed After Installation?
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**
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	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**

Parameter	Description	Can Entry Be Changed After Installation?
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.	Yes, you can change the entry after installation by using the Cisco Unified Communications Operating System: **Settings** > **NTP Servers**
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:	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.	Yes, you can change the entry after installation by using the following CLI command: **CLI** > **set password security**
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**

Parameter	Description	Can Entry Be Changed After Installation?
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**
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**

Obtain license file

Licensing helps manage Cisco Unified Communications Manager Business Edition 5000 licenses and enforces the licenses for Cisco Unified Communications Manager Business Edition 5000 applications and the number of IP phones. This section provides information on obtaining licenses for the Cisco Unified Communications Manager portion of a Cisco Unified Communications Manager Business Edition 5000 system. For information on licensing for the Cisco Unity Connection portion of the system, see the *System Administration Guide*.

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.

Obtain license file for new servers and devices

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

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 Cisco Unified Communications Manager Business Edition 5000 server. You must enter a valid e-mail address as well as the number of 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.

Step 4 You must upload the license file to the server with the matching MAC address that you provided in the previous step.

This server then takes on the functionality of the license manager.

Related Topics

Install licenses

Answer file generator

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

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.

Install new operating system and application

This section describes how to install the operating system and the Cisco Unified Communications Manager Business Edition 5000 application. You install the operating system and application by running one installation program.

Installation wizard

For instructions on how to navigate within the installation wizard, see the following table.

Table 3: Installation wizard navigation

To Do This	Press This
Move to the next field	Tab
Move to the previous field	Alt-Tab

To Do This	Press This
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)

Install software

To start the installation, follow this procedure.

Note Because the Cisco Unified Communications Manager Business Edition 5000 software was preinstalled on the server, you do not need to reinstall the software unless you want to reimage the server with a later product release. Go directly to the procedure to enter the configuration information.

Procedure

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

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 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.

  Note If one or more products are not supported on your server, that information also appears. If or Cisco Unified Communications Manager Business Edition 5000 is listed as not supported on your server, confirm that the server meets Connection 7.x specifications. See the applicable table for your server model in the *Cisco Unity Connection Supported Platforms List* at http://www.cisco.com/en/US/products/ps6509/products_data_sheets_list.html.

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 the applicable option:

- If Cisco Unity Connection or Cisco Unified Communications Manager Business Edition 5000 software is already installed on the server, click **Skip**, and perform the procedure to enter the configuration information.
- If you want to perform a standard installation, click **Proceed**, and continue with this procedure.
- If you want to perform an unattended installation, click **Skip**, and perform the procedure to enter the configuration information. For an unattended installation, you provide preexisting configuration information on a USB key or floppy disk.
- If you want to install the software now and configure it later, click **Skip**, and perform the procedure to enter the configuration information. This installation method may take more time than other methods.

Step 9 Choose the type of installation to perform by doing the following steps.
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 to perform the procedure to apply a patch.
- 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 to perform the basic software installation procedure.

Related Topics

Apply a patch, on page 19
Basic software installation, on page 22
Enter preexisting configuration information, on page 18

Enter 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.
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 to perform the procedure to apply a patch.
- To skip this step, choose **No.**
- To return to the previous window, choose **Back.**

Step 5 In the Basic Install window, choose **Continue**. Continue to perform the basic software installation procedure.

Related Topics

Apply a patch, on page 19
Basic software installation, on page 22

Apply 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.

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 Upgrade from a remote server.
- FTP - Retrieves the upgrade file from a remote server by using File Transfer Protocol (FTP). Skip to the Upgrade from a remote server.
- LOCAL - Retrieves the upgrade file from a local DVD. Continue with the Upgrade from a local disk, on page 19.

Upgrade 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 the next step.

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 Basic software installation.

Upgrade 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.

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://www.cisco.com/pcgi-bin/ctdp/Search.pl. 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. Skip the next step then continue.

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

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 server 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.
- If you want to configure static IP addresses for the server, 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 Installation information 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 Installation information 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 the next step.

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 Basic software installation.

Basic software 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**.

  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 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 server 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.
- If you want to configure a static IP address for the server, 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 Installation information 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 Installation information 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 Installation information.

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.**

Step 10 Continue with the Set up first node.

Set up server

After you finish the basic installation, follow this procedure to configure the server.

Procedure

Step 1 The Network Time Protocol Client Configuration window displays.
Cisco recommends that you use an external NTP server to ensure accurate system time on the publisher server. Ensure the external NTP server is stratum 9 or higher (meaning stratums 1-9). The subscriber server will get its time from the publisher 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 Installation information.
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 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 Installation information 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.

Post-installation tasks

After installing the Cisco Unified Communications Manager Business Edition 5000 on your server, you must perform some post-installation tasks before you can begin using it. See the following table for post-installation tasks that you must complete after the installation.

Note To access web applications, you must use a web browser from a computer that has network access to the Cisco Unified Communications Manager Business Edition 5000 server.

Table 4: Post-Installation Tasks

Post-Installation Tasks	Important Notes
Log in as the Cisco Unified Communications Manager or Cisco Unity Connection Application User and change the Application User passwords.	See the Change default application user passwords.
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*.
Upload your license files to the server.	See the Install licenses.
Activate Cisco Unified Communications Manager and Cisco Unity Connection 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 Services activation, on page 26.
Configure the backup settings. Remember to back up your 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*. To download and install additional Cisco Unity Connection language files, see the *Installation Guide for Cisco Unity Connection* Release 8.x at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/installation/guide/8xcucigx.html.
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*.
Configure the system.	See theSet up database, on page 27. For more information, refer to the *Cisco Unified Communications Manager System Guide*.

Post-Installation Tasks	Important Notes
Install Cisco Unified CM with IM and Presence service.	See Installation overview.

Change 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 Cisco Unity Connection Administration and change these passwords. See *Cisco Unified Communications Manager Administration Guide* and the *System Administration Guide for Cisco Unity Connection* for the procedures for changing passwords.

Services activation

Even though all services are installed on the server, you may need to use Cisco Unified Serviceability to manually activate services that you want to run. For service recommendations and more information, see *Cisco Unified Serviceability Administration Guide* .

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 Licensing. The Cisco Unified Communications Manager server where the license file is loaded takes on the functionality of the license manager.

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*.

Set up 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.

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

Command Syntax

file list install *

To view the log file from the command line, enter

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:

- *Cisco Unified Real Time Monitoring Tool Administration Guide*
- *Troubleshooting Guide*