



Pre-Install

Introduction

In this section you will use the Pre-Upgrade Checklist to complete all the tasks necessary before you actually do the upgrade.

Before You Begin

You should have completed the Minimum Skills/Knowledge Checklist.

When You Are Done

You will have completed the Pre-Upgrade Checklist. Go on to Install.

Pre-Upgrade Checklist

Perform the following tasks before you begin the upgrade. Clicking a link in the “Task Details” column opens the referenced procedure in a popup window. Notes indicate where there are other sections of the referenced document important for background information or context.

	Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/>	Step 1 Verify that your system meets the system requirements for upgrading Cisco Unified Communication Manager nodes in the cluster.	To find which servers support Cisco Communication Manager 5.x releases, refer to the Guide to Cisco Communication Manager Upgrades and Server Migrations at http://www.cisco.com/en/US/partner/products/hw/voiceapp/ps378/prod_brochure_list.html .
<input type="checkbox"/>	Step 2 Run Cisco Unified Communication Manager Upgrade Utility on the server to verify that the system is ready for upgrade.	Refer to <i>Using Cisco Unified Communication Manager Upgrade Utility</i> . Note Review the document to install the utility and to understand what checks the utility performs.

Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/> Step 3 Perform the recommended backup procedures on the publisher server. Back up every database that is associated with your Cisco Unified Communication Manager server.	<p>Refer to <i>Cisco IP Telephony Backup and Restore System (BARS) Administration Guide</i>.</p> <p>Note Review the document overview for information on the versions of applications that BARS supports and for instructions on installing BARS.</p>
<input type="checkbox"/> Step 4 If you are using a third-party application to access Call Detail Records (CDR), perform a backup of the CDR data as recommended in the third-party vendor documentation.	<p><i>Cisco IP Telephony Backup and Restore System (BARS) Administration Guide</i>.</p> <p>Note Review the document overview for information on the versions of applications that BARS supports and for instructions on installing BARS.</p>
<input type="checkbox"/> Step 5 If you do not need to carry over your CDR data to Cisco Unified Communication Manager 5.1(1), Cisco recommends that you purge the CDR data before you run DMA.	<p>Purging the CDR data speeds up the migration process and decreases the size of the DMA TAR file.</p> <p>Purging CDR: Refer to “Using Manual Database Purge” in <i>Cisco CallManager Serviceability Administration Guide, Release 4.1(3)</i>.</p>
<input type="checkbox"/> Step 6 (If your systems are using centralized TFTP) Upgrade off-clusters in the centralized TFTP environment.	<p>When upgraded to 5.x, the other clusters participating in Centralized TFTP must be running a supported version (see list below) of Cisco Unified CM.</p> <p>Configuring Centralized TFTP: Refer to “Cisco TFTP” in the <i>Cisco Unified CallManager System Guide 5.0(4)</i></p> <p>Note The referenced procedure in the 5.0(4) System Guide applies to 5.1(1) as well.</p> <p>Supported versions of Cisco Unified CM:</p> <ul style="list-style-type: none"> • 3.3(5)sr2 • 4.1(3)sr2 • 4.2 • 4.3 • 5.0 • 5.1 • 6.0 <p>These Cisco Unified CM versions are not supported:</p> <ul style="list-style-type: none"> • 4.0(1) • 4.0(2) • 4.1(1) • 4.1(2)

	Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/>	<p>Step 7 Export the data on the current Cisco Unified Communication Manager Publisher server by running the Data Migration Assistant (DMA).</p> <p>Ensure the configuration files and exported data files are located in one of the following locations:</p> <ul style="list-style-type: none"> • Hard drive (for DMABackupInfo.inf only) • Floppy drive (for DMABackupInfo.inf only) • Tape drive • Remote drive <p>Note Running DMA is required for obtaining the license file (see Checklist for Upgrading the First Cisco Unified CM Node).</p>	<p>DMA generates two files:</p> <ul style="list-style-type: none"> • A tape archive (TAR) file that contains the database and directory information. The format of the filename follows: DMABackup<M>-<D>-<Y>#<H>-<mm>.tar where M specifies the month, D specifies the day, Y specifies the year, H specifies the hour in a 24-hour format, and mm specifies the minutes. • A backup information file that contains Cisco Unified Communication Manager configuration data, named DMABackupInfo.inf. The system saves it in the D:\DMA folder as part of the TAR file. <p>Note Do not change the configuration data filename. The upgrade fails if it does not find a file with the exact filename and format.</p> <p>For more information on data migration, refer to <i>Data Migration Assistant Administration Guide</i>. You will be choosing an installation option based on the location of the DMA output configuration file and TAR file.</p> <p>Note Review the pre installation guidelines and installation procedures</p>
<input type="checkbox"/>	<p>Step 8 Before the upgrade, obtain the necessary information for configuring the platform and Cisco Unified CM on the first and subsequent nodes.</p>	<p>See the “Installation Information Worksheet” section on page 2-4.</p>
<input type="checkbox"/>	<p>Step 9 Record the Host Name/IP Address value that is configured on the Server Configuration Settings window of the Cisco Unified CallManager 4.x server.</p>	<p>To access the Host Name/IP Address field on the 4.x server, navigate to System > Server.</p> <p>For more information, see Assigning the Host Name or IP Address to the Server</p>
<input type="checkbox"/>	<p>Step 10 Match the server’s NIC speed and duplex settings with the switch port’s configuration. For servers or switch ports that can support GigE (1000BaseT), use auto-negotiation on both sides.</p>	<p>For more information, see “NIC and Switch port Speed and Duplex” in Installation Field Definitions.</p>
<input type="checkbox"/>	<p>Step 11 Enable PortFast on all switch ports connected to Cisco Unified servers.</p>	<p>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 a port waits before changing from its Spanning-Tree Protocol (STP) learning and listening states to the forwarding state.</p>

	Pre-Upgrade Task	Task Details (Links) and Notes
<input type="checkbox"/>	Step 12 (If you are using NIC teaming) Be aware that the NIC teaming configuration will be lost during the upgrade. You will need to set it up on each server after the upgrade.	After the upgrade, be sure to complete Step 1 in the Post-Upgrade Checklist.
<input type="checkbox"/>	Step 13 Familiarize yourself with the navigation options within the installation wizards.	See Navigating Within the Installation Wizard.

Installation Information Worksheet

Use Table 2-1 to record the information about your Cisco Unified Communication Manager server. Gather this information for each Cisco Unified Communication 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 can 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

Alternatively, download and use a Microsoft Word version of the worksheet.



Note

Because some of the fields are optional, they may not apply to your configuration. For example, you choose not to set up an SMTP host.



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 a field can be changed after installation, and if so, whether you can change it through platform administration or through the Command Line Interface (CLI).

Table 2-1 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Administrator Password		Yes. CLI > set password admin
Application User Password		Yes CLI: set password
Country		Yes CLI> set web-security
DHCP		Yes CLI> set network dhcp
DNS Primary		Yes CLI> set network dns

Table 2-1 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
DNS Secondary		Yes CLI> set network dns
Domain		Yes CLI> Set Network Domain
Domain Name Service DNS Enable		No
Gateway Address		Yes. Use Platform Administration > Settings>IP or CLI > set network gateway
Host Name		No
IP Address		Yes Use Platform Administration > Settings>IP or CLI> set network IP
IP Mask		Yes. Use Platform Administration > Settings>IP or CLI > set IP
Location		Yes CLI> set web-security
Master Administrator ID		No
NTP Server IP Address Note You can enter up to five NTP servers.		Yes Use Platform Administration > Settings>NTP Servers
Organization		Yes CLI> set web-security
Security Password		Yes CLI> set password security
SMTP Location		Yes CLI> set smtp
State		Yes CLI> set web-security

Table 2-1 Configuration Data

Configuration Data	Your Entry	Can Entry Be Changed After Installation
Time Zone		Yes CLI> Set Timezone
Unit		Yes CLI> set web-security
End-User Password		Yes See “End User Configuration” in the <i>Cisco Unified Communication Manager Administration Guide</i> .
End-User PIN		Yes See “End User Configuration” in the <i>Cisco Unified Communication Manager Administration Guide</i> .

For more detailed descriptions of each installation field, see Table 2-2.

Table 2-2 Installation Field Definitions

Field	Description	Usage
Administrator ID	This field specifies the name that you want to assign to this account.	Ensure the name is unique; it can contain lowercase, alphanumeric characters, hyphens, and underscores. It must start with a lowercase alphanumeric character. For this mandatory field, you should record it for use when you log in to the CLI on the platform or into Platform Administration. Note You cannot change this field after installation.
Administrator Password	This field specifies the password that you use for logging in to the CLI on the platform and for logging in to Cisco Unified Communications Operating System Administration.	Ensure the password is at least six characters long; it can contain alphanumeric characters, hyphens, and underscore. For this mandatory field, you should record it for use when you log in to the Cisco Unified CallManager.

Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
DHCP	Dynamic Host Configuration Protocol	Choose Yes if you want to use DHCP to automatically configure the network settings on your server. If you choose No , you must enter a hostname, IP Address, IP Mask, and Gateway.
DNS Enabled	A DNS server represents a device that resolves a hostname into an IP address or an IP address into a hostname. Note You cannot change the DNS settings after the installation is complete. To change DNS settings, you must reinstall Cisco Unified Communication Manager.	If you do not have a DNS server, enter No . When DNS is not enabled, you should only enter IP addresses (not hostnames) for all network devices in your Cisco Unified Communications network. If you have a DNS server, Cisco recommends entering Yes to enable DNS. Disabling DNS limits the system ability to resolve some domain names.
DNS Primary	Cisco Unified Communication Manager contacts this DNS server first when it attempts to resolve host names.	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 where ddd can have a value between 0 and 255 (except 0.0.0.0). Consider this field mandatory if DNS is set to yes .
DNS Secondary	When a primary DNS server fails, Cisco Unified Communication Manager will attempt to connect to the secondary DNS server.	In this optional field, enter the IP address of the secondary DNS. Enter the IP address in dotted decimal format as ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0).
Domain	This field represents the name of the domain in which this machine is located.	Consider this field mandatory if DNS is set to yes .
First Cisco Unified Communication Manager Node	The first Cisco Unified Communication Manager node contains the database. Subsequent nodes connect to the the first node to access database content. The first node also synchronizes with an external NTP server and provides time to the other nodes.	Choose Yes if you are configuring the first Cisco Unified Communication Manager node in the cluster. If you are configuring subsequent nodes, see Table 2-2 for information on the different fields.


Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
Gateway Address	A gateway represents a network point that acts as an entrance to another network. Outbound packets get sent to the gateway that will forward them to their final destination.	Enter the IP address of the gateway in the format ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0) If you do not have a gateway, you must still fill in this field by setting it to 255.255.255.255. Not having a gateway may limit you to communicating only with devices on your subnet.
Hostname	A host name represents an alias that is assigned to an IP address to identify it.	Enter a host name that is unique to your network. The host name can comprise up to 64 characters and can contain alphanumeric characters and hyphens. If DHCP is set to No , consider this field mandatory.
IP Address	This field specifies the IP address of this machine. It will uniquely identify the server on this network. Another machine in this network should not be using this IP address.	Enter the IP address in the form ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). If DHCP is set to No , consider this field mandatory.
IP Mask	This field specifies the IP subnet mask of this machine. The subnet mask together with the IP address defines the network address and the host address.	Enter the IP mask in the form ddd.ddd.ddd.ddd where ddd can have a value between 0 and 255 (except 0.0.0.0). A valid mask should have contiguous '1' bits on left side and contiguous '0' bits on the right. For example, a valid mask follows: 255.255.240.0 (11111111.11111111.11110000.00000000) An invalid mask follows: 255.255.240.240 (11111111.11111111.11110000.11110000)

Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
NIC and Switch port Speed and Duplex	<p>NIC Speed specifies the speed of the server network interface card (NIC) in megabits per second.</p> <p>NIC Duplex specifies the duplex setting of the server NIC.</p>	<p>Speed: 10, 100, or 1000</p> <p>Duplex: Half or full.</p> <p>Note For GigE (1000/FULL), NIC and switch port settings must be handled differently than they were in Windows, where setting hard values and not using Autonegotiation was strongly recommended. For Linux-based Cisco Unified CM 5.x, set the NIC and switch port to Auto/Auto for 1000/FULL operation. Do not set hard values. The NIC and switch port sides must both be set to Auto.</p> <p>Note If you are using NIC Teaming, be aware that the NIC Teaming configuration will be lost during the upgrade. You will need to set it up on each server after the upgrade. After the upgrade, see NIC teaming in the Post-Upgrade Checklist.</p>
NTP Server	This field identifies the NTP server with which you want to keep time synchronization.	<p>Enter the hostname or IP Address of NTP server(s).</p> <p>If you enabled the system to be NTP client, you must enter the hostname or IP address of at least one NTP server.</p> <p>Note You can add additional NTP servers or make changes to the NTP server list at a later time</p>

Table 2-2 Installation Field Definitions (continued)

Field	Description	Usage
Security Password	<p>Cisco Unified Communication Manager servers in the cluster use the security password to communicate with one another.</p> <p>You will be asked to enter the same security password for each subsequent node in the cluster.</p>	<p>Enter the security password.</p> <p>Enter the same password in the confirm password field.</p> <p>The password must contain at least six alphanumeric characters. It can contain hyphens and underscores, but it must start with an alphanumeric character.</p> <p> Caution You must enter the same password for all nodes in the cluster.</p>
Set Hardware Clock	<p>The field specifies the date and local time for the machine.</p> <p>Note If you set the hardware clock manually, the node does not use an external NTP server for time synchronization.</p>	<p>Choose Yes if you want to set the date and local time for the time zone that you chose.</p> <p>Enter the hours based on a 24-hour format.</p> <p>Note If you configure an external NTP server, the hardware clock gets set automatically.</p>
SMTP	<p>This field specifies the name of the SMTP host that is used for outbound e-mail.</p>	<p>Enter the hostname or dotted IP address for the SMTP server. For a host, it can contain alphanumeric characters, hyphens, or periods. For a host name, it must start with an alphanumeric character.</p> <p>You must fill in this field if you plan to use electronic notification. If not, you can leave it blank.</p>
Time zone	<p>This field specifies the local time zone and offset from Greenwich Mean Time (GMT)</p>	<p>Choose Yes if you want to change the time zone.</p> <p>Choose the time zone that most closely matches the location of your machine.</p>

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, a message displays, and you are 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)**—Allows you to review and modify the networking configuration. The installation program returns to the network configuration windows.

Networking is validated after you complete each networking window, so the message might display multiple times. If the message displays while you are reviewing the network configuration windows, choose **IGNORE** to move to the next window. If you choose **REVIEW**, the first network configuration window appears again.

- **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.

Related Training

Please check back for updated training links.

