Installing Cisco Unified Contact Center Express Release 8.0(x)

For Cisco Unified Contact Center Express and Cisco Unified IP IVR Releases 8.0(1) and 8.0(2)

The Cisco Unified Contact Center Express (Unified CCX), Release 8.0(x) uses a different installation framework than previous releases of Unified CCX. Review all installation instructions carefully prior to installing Unified CCX 8.0(x).

This document explains how to install Unified CCX 8.0(x) on a single node setup (Standalone) or two-node setup (High Availability) in a cluster environment.

For information about upgrading from a previous release (5.0(2) or 7.0(1) release) of Unified CCX to the current appliance version, which is 8.0(x), see *Upgrade Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html

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

Contents

This guide contains the following topics:

Overview

Unified CCX provides a single, consistent, and easy-to-manage platform for the following products:

- Unified CCX
- Unified IP IVR

This document provides instructions and related information for installing, reinstalling, and patching Unified CCX 8.0(x), and for performing initial setup tasks.

Note For more information on how to upgrade from your existing Unified CCX 8.0(1) to 8.0(2) version, see the *Release Notes for Cisco Unified CCX and Cisco Unified IP IVR, Release 8.0(2)* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_release_notes_list.html

Audience

This guide is intended for Cisco Unified Communications system administrators. You should have the network and telephony knowledge that is required to install and set up the Unified CCX software. You should also be familiar with the Cisco Unified Communications Manager (Unified CM) or Cisco Unified Communications Manager Express (Unified CME) configurations at your site.

Related Documentation

For additional installation-related information, see the following documents:

- *Upgrade Guide for Cisco Unified CCX and Cisco Unified IP IVR*
  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html
- *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*
  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
- For a list of troubleshooting tips related to installation, see the folloiwng URL:
  http://docwiki.cisco.com/wiki/Troubleshooting_Unified_Contact_Center_Express
- For a complete list of terms used in Cisco Unified CCX and Cisco Unified IP IVR, see the following URL
  http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_technical_reference_list.html

For further information about Unified CCX documentation, see the following URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/tsd_products_support_series_home.html

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 the Second Node
- Apply a Patch During Installation of the First Node
- Apply a Patch During Installation of the Second Node
- Add and Configure the Second Node for HA

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.

Install Software from a DVD on the First Node

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

Table 1 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 "Performing Pre-Installation Tasks" section on page 9.
Step 2	Follow the procedure to begin installing the software on the DVD to your server.	See the "Starting the Installation" section on page 31.
Step 3	Follow the procedure for performing a basic installation.	See the "Performing the Basic Installation" section on page 42.
Step 4	When the First Node Configuration window displays, choose **Yes** to configure the new server as the first node.	See Step 9 in the "Performing the Basic Installation" section on page 42.

Table 1 Installing Software from a DVD on the First Node

	Task	For More Information
Step 5	Follow the procedure to configure the first node.	See "Configuring the First Node" section on page 49.
Step 6	Follow the procedure to perform the initial setup configuration for the first node and perform other post-installation tasks that apply to your site.	See the "Performing Initial Setup for the First Node" section on page 63. For a list of post-installation tasks, see Table 10 on page 62.

Install Software from a DVD on the Second Node

To install software from a DVD on the second node, follow the steps in Table 2.

Table 2 Installing Software from a DVD on the Second 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 "Performing Pre-Installation Tasks" section on page 9.
Step 2	Follow the procedure to add the second node to the first node.	See "Adding the Second Node for HA" section on page 56.
Step 3	Follow the procedure to begin installing the software on the DVD to your server.	See "Starting the Installation" section on page 31.
Step 4	Follow the procedure for performing a basic installation.	See "Performing the Basic Installation" section on page 42.
Step 5	When the First Node Configuration displays, choose **No** to configure the new server as the second node for high availability (HA).	See Step 9 in the "Performing the Basic Installation" section on page 42.

Table 2 Installing Software from a DVD on the Second Node

	Task	For More Information
Step 6	Follow the procedure to configure the second node and form a cluster.	See the "Configuring the Second Node for HA" section on page 57.
Step 7	Follow the procedure to perform the initial setup configuration for the second node and perform other post-installation tasks that apply to your site.	See the "Performing Initial Setup for the Second Node" section on page 73. For a list of post-installation tasks, see Table 10 on page 62.

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 3.

Table 3 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 "Performing Pre-Installation Tasks" section on page 9.
Step 2	Follow the procedure to begin installing the software on the DVD to your server.	See "Starting the Installation" section on page 31.
Step 3	Follow the procedure to apply a software patch.	See "Applying a Patch" section on page 38.
Step 4	Follow the procedure for performing a basic installation.	See "Performing the Basic Installation" section on page 42.
Step 5	When the First Node Configuration window displays, choose **Yes** to configure the new server as the first node.	See Step 9 in the "Performing the Basic Installation" section on page 42.
Step 6	Follow the procedure to configure the first node.	See the "Configuring the First Node" section on page 49.
Step 7	Perform all post-installation tasks that apply to your site.	For a list of post-installation tasks, see Table 10 on page 62.

Apply a Patch During Installation of the Second 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 4.

Table 4 Applying a Patch During Installation of the Second 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 "Performing Pre-Installation Tasks" section on page 9.
Step 2	Follow the procedure to begin installing the software on the DVD to your server.	See "Starting the Installation" section on page 31.
Step 3	Follow the procedure to apply a software patch.	See "Applying a Patch" section on page 38.
Step 4	Follow the procedure for performing a basic installation.	See "Performing the Basic Installation" section on page 42.
Step 5	When the First Node Configuration window displays, choose **No** to configure the new server as the second node.	See Step 9 in the "Performing the Basic Installation" section on page 42.
Step 6	Follow the procedure to configure the second node and form a cluster.	See the "Configuring the Second Node for HA" section on page 57.
Step 7	Perform all post-installation tasks that apply to your site.	For a list of post-installation tasks, see Table 10 on page 62.

Add and Configure the Second Node for HA

To add the second node for HA, follow the steps in Table 5.

Table 5 Adding the Second Node for HA

	Task	For More Information
Step 1	Before you make any changes to a cluster, be sure that you have a current backup file.	For more information, see the *Disaster Recovery System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
Step 2	Perform all pre-installation tasks that apply to your site.	For a list of pre-installation tasks, see "Performing Pre-Installation Tasks" section on page 9.
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, see the *Upgrade Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_installation_guides_list.html
Step 4	Before you install the new node, ensure that you have added it to the first node. From the Cisco Unified CCX Administration of the first node, add the IP address/Hostname of the second node.	See "Adding the Second Node for HA" section on page 56.
Step 5	Record the configuration settings for the server that you plan to install.	To record your configuration settings, see Table 7 on page 18.
Step 6	You must install the same software version on both nodes in the cluster.	For more information on the different installation options, see the "Installation Overview" section on page 29.
Step 7	Follow the procedure to begin installing the software on the DVD to your server.	See "Starting the Installation" section on page 31.

Table 5 Adding the Second Node for HA

	Task	For More Information
Step 8	If you need to upgrade the version of Unified CCX, continue with the procedure for applying a software patch.	See "Applying a Patch" section on page 38.
Step 9	Follow the procedure for performing the basic installation.	See "Performing the Basic Installation" section on page 42.
Step 10	When the First Node Configuration displays, choose **No** to configure the new server as the second node.	See Step 9 in the "Performing the Basic Installation" section on page 42.
Step 11	Follow the procedure to configure the second node and form a cluster.	See the "Configuring the Second Node for HA" section on page 57.
Step 12	Follow the procedure to perform the initial setup configuration for the second node and perform other post-installation tasks that apply to your site.	See the "Performing Initial Setup for the Second Node" section on page 73. For a list of post-installation tasks, see Table 10 on page 62.

Performing Pre-Installation Tasks

This section contains the important considerations, frequently asked questions, and pre-installation tasks that you need to perform to ensure that you can successfully install Unified CCX.

Planning to Install Unified CCX

Unified CCX is the backbone of the Cisco Unified Contact Center environment, comprising:

- **The first node**. Required in all deployments of Unified CCX.
- **The second node**. The second node provides fault tolerance to the system and provides standby capabilities if the first node goes down. The second node, also called high availabiilty (HA) node is optional. The first and second nodes can be split across the local area network (LAN) and wide area network (WAN).

Unified CCX 8.0(x) is an appliance application similar to Unified CM. It must be installed on dedicated servers, which must be Media Convergence Servers (MCS). For details on the server requirements, see "Server Requirements" section on page -11.

Important Considerations

Carefully read the information that follows before you proceed with the installation:

- Installing Unified CCX 8.0(x) on an existing server will format the hard drive and permanently remove the existing Unified CCX data. It also upgrades the system Basic Input Output System (BIOS), firmware, and Redundant Array of Inexpensive Disks (RAID) configuration if found outdated.
- Ensure to connect each Unified CCX node to an uninterruptible power supply (UPS) to protect Unified CCX server from unexpected power failure that may damage the physical media and to avoid reinstallation of Unified CCX.
- Install the Unified CCX software on the first node or publisher node first and then on the second node.
- Verify that the first node is reachable (via LAN or WAN) from the second node before you start installing the second node.
- Make a note of the security password that you specified while installing the first node as it is required during the installation of second node.
- If you plan to install the Unified CCX software without DNS information, then make sure you provide only the IP Address as reference instead of host names.
- Configure the server by using a static IP address so that the server IP address remains unchanged.
- During installation, field values (namely host name and passwords) entered on the configuration wizard are case-sensitive.
- Use the same Maximum Transmission Unit (MTU) value for all servers in the cluster.
- Cisco Unified CCX does not support Interface Bonding (NIC teaming).

- If you are already running CRS 5.x or Unified CCX 7.x and planning to install Unified CCX 8.0(x), use the Cisco Unified CCX Pre-Upgrade Tool to back up all of the data from your existing system and restore this data on the upgraded Unified CCX 8.0(x) system.
- To remove any Unified CCX version, an MCS server must be reimaged. Before you start reimaging a server, back up the existing Unified CCX data from the server to avoid permanent loss of data. Unified CCX 8.0(x) does not support uninstallation.
- Install the Unified CCX software during off-peak hours or a maintenance window to avoid interruptions.

Installation Requirements, Prerequisites, and Related Procedures

Server Requirements

Unified CCX 8.0(x) is packaged with the Linux-based Unified Communications Operating System (UCOS). It is an appliance model developed by Cisco. This appliance model provides a collection of frameworks, such as installation, serviceability, service management, etc. so that Unified CCX installed on this platform can leverage more out of this in terms of integration, communication and administration in coordination with Unified Communications Manager (Unified CM) or Unified Communications Manager Enterprise (Unified CME).

Note Cisco Unified CCX does not support Interface Bonding (NIC teaming).

To install Unified CCX on approved servers (MCS, B-series, and C-series), following hardware requirements must be met.

- Hardware—Approved MCS, B-series, and C-series servers
- Hard disk—146 GB minimum
- RAM—2 GB minimum

For a list of approved MCS, B-series, and C-series servers, see the *Software and Hardware Compatibility Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html

Note To prevent unpredictable behavior or loss of Unified CCX configuration and user data due to power failure, ensure uninterrupted power supply to the Unified CCX servers at all times.

Client System Requirements

You can access the Cisco Unified CCX 8.0(x) Administration Web interface from a remote system using a Web browser, having access to your network. A remote system must meet the following minimum hardware requirements:

- Windows XP Professional with Service Pack 2/3, or Windows Vista Business/Ultimate
- 500 MHz Intel Pentium
- 512 MB RAM
- 650 MB available disk space
- 100 MB (Fast Ethernet) Network Interface card (NIC)
- 800x600 screen resolution

Browser Requirements

You can access Cisco Unified CCX Administration Web interface using the following browsers:

- Microsoft Internet Explorer version 6.x or later
- Mozilla Firefox version 2.0 or later

Cisco does not support or test on any other Web browsers.

Obtaining License for Unified CCX 8.0(x)

Licensing helps manage Unified CCX licenses and enforces the licenses for Unified CCX components and nodes. In Unified CCX 8.0(x), all the licenses are node-locked, which means the use of the license is restricted to only one particular

node based on the License MAC Address of that node. Typically, a Unified CCX 8.0(x) license is based on the License MAC of the first node only. This section provides information on obtaining licenses for new Unified CCX nodes as well as for Unified CCX nodes that have been upgraded from various releases.

Use Demo Licenses

The Unified CCX 8.0(x) Installation DVD comes bundled with four demo licenses; one each for Unified IP IVR, STD, ENH, and PRE package. Since ordering actual licenses may take a while, you can start using the demo licenses by uploading them to the system using the Unified CCX 8.0(x) Web Administration. A demo license is valid for initial 30 days only. You can use these demo licenses to get a feel of capabilities of the applications available on the Unified CCX 8.0(x) Installation DVD during the initial 30 days. Using the demo licenses helps you decide on the capabilities expected from each package.

Obtain License MAC

The Unified CCX 8.0(x) system uses a new licensing mechanism. The licenses are based on a string called the License MAC which is different from the physical MAC address of a system. The License MAC string is generated during installation and is based on various input fields, such as the hostname, IP address, etc. If any of these fields change after fresh installation, the License MAC will become invalid and you must request new license(s). You can generate the License MAC in one of the following ways.

- Obtain License MAC after installing Unified CCX 8.0(x), page 13
- Obtain License MAC before installing Unified CCX 8.0(x), page 14

Obtain License MAC after installing Unified CCX 8.0(x)

License MAC will be displayed during system install. You must make a note of this for ordering license files. To obtain License MAC after installing Unified CCX 8.0(x), complete the following steps:

Step 1 Log in to the Unified CCX 8.0(x) system command line interface (CLI) using Unified CCX Administrator credentials.

Step 2 Run “show status” command. Output of this command contains the License MAC.

Obtain License MAC before installing Unified CCX 8.0(x)

To obtain License MAC prior to installing Unified CCX 8.0(x), complete the following steps:

Step 1 Go to the answer file generation Web site.
http://www.cisco.com/web/cuc_afg/index.html

Step 2 Select **Cisco Unified CCX** from **Product Options**.

Step 3 Fill in all the configuration information used for installation, such as IP address, hostname, and more on that site.

Answer file generated from this can be used for unattended Unified CCX 8.0(x) installation. You can also use this answer file to generate the License MAC (based on given parameters) so you can order the license prior to building the machine.

Step 4 Once the answer file is generated, this page enables you to obtain the License MAC.

Caution If you change any of the parameters or configuration information after ordering the license, License MAC will be changed and the ordered license file may become invalid.

To obtain a node license file for new Unified CCX servers and to obtain additional node-locked licenses, complete the following steps:

Step 1 Enter the Product Authorization Key (PAK) that you received with your Unified CCX 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 License MAC of the first node of the Unified CCX cluster. You must enter a valid e-mail address as well as the number of nodes for which you want licenses.

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 **uccx_80_<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 Unified CCX 8.0(x) supports only node-locked licenses. However, Unified CCX 8.0(x) continues to recognize the existing licenses used for Unified CCX versions earlier than 8.0(x) on an upgraded system. This feature is currently available for Unified CCX in Standalone setup only.

Step 4 You must upload the license file to the server with the matching License MAC address that you provided in Step 3. This server then takes on the functionality of the license manager.

For more information on how to upload a license file and view license information, see the *Administration Guide Cisco Unified CCX and Cisco Unified IP IVR* available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html.

Step 5 For Unified CCX HA setup, a Warm Standby License is issued to enable this feature. The process of ordering such a license is the same as that of a single node Standalone license.

The Unified CCX 8.0(x) Warm Standby license and all other licenses are node-locked to the License MAC Address of the first node (typically the Database Publisher node) of a Unified CCX cluster. When a second node is added, it is verified that the first node has the valid add-on Warm Standby License. Once the cluster is set up, the licenses will be valid on both the nodes in a cluster.

License MAC is dependent on some system parameters. Modifying any of these parameters can change License MAC thereby invalidating current License files. Here are the parameters on which the validity of a License MAC depends:

- Time zone
- NTP server 1 (or ‘none’)
- NIC speed (or ‘auto’)
- Hostname

- IP Address
- IP Mask
- Gateway Address
- Primary DNS
- SMTP server
- Certificate Information (Organization, Unit, Location, State, Country)

Licensing Grace Period

In case your License MAC becomes invalid, you must request new license(s). The system however continues to operate for 30 days without a new license. After the 30-days grace period ends, the system will shut down until you upload a new license using the updated License MAC. Once you obtain re-hosted licenses, these licenses can be uploaded through Add License page of the Unified CCX 8.0(x) Administration Web interface.

Cisco Unified CCX Disk Space Usage

This section provides information about determining disk space usage and requirements when you install Cisco Unified CCX. The historical reporting (HR) database (DB) size of Cisco Unified CCX depends on the size of the hard disk on which it is stored. Table 6 provides an example of disk space usage for these DB types.

Table 6 Cisco Unified CCX Disk Space Usage Examples

Server Generation	Server Type	Server Disk Size	HR DB Size	Repository DB Size	Agent DB Size (rascal)	Configuration DB Size
Nantucket	7835	2x146 GB	13 GB	3.0 GB	0.5 GB	0.5 GB
	7845	4x146 GB	20 GB	3.0 GB	0.5 GB	0.5 GB
Barnstable	7816	1x160 GB	11 GB	3.0 GB	0.5 GB	0.5 GB
	7825	2x160 GB	12 GB	3.0 GB	0.5 GB	0.5 GB

Table 6 Cisco Unified CCX Disk Space Usage Examples

Server Generation	Server Type	Server Disk Size	HR DB Size	Repository DB Size	Agent DB Size (rascal)	Configuration DB Size
Rockport	7816	1x250 GB	11 GB	3.0 GB	0.5 GB	0.5 GB
	7825	2x250 GB	12 GB	3.0 GB	0.5 GB	0.5 GB
	7835	2x146 GB	13 GB	3.0 GB	0.5 GB	0.5 GB
	7845	4x146 GB	20 GB	3.0 GB	0.5 GB	0.5 GB
Portsmouth 1	7835	2x146 GB	13 GB	3.0 GB	0.5 GB	0.5 GB
	7845	4x146 GB	20 GB	3.0 GB	0.5 GB	0.5 GB
	7845	4x300 GB	26 GB	3.0 GB	0.5 GB	0.5 GB
	7855	4x300 GB	26 GB	3.0 GB	0.5 GB	0.5 GB
Portsmouth 2	7816	1x250 GB	11 GB	3.0 GB	0.5 GB	0.5 GB
	7825	2x250 GB	12 GB	3.0 GB	0.5 GB	0.5 GB

Gathering Configuration Information for Installation

Use Table 7 to record the information about your server that both the Answer File Generator and the basic installation wizard prompt you to enter. Gather this information for each Unified CCX 8.0(x) server that you install. 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 so it is easy 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 CLI command.

Caution Changing some of these configuration parameters result in changes to your current License MAC. In such as case, you need to rehost the Unified CCX 8.0(x) license(s). For more information, see "Obtain License MAC" section on page 13.

Table 7 Node Configuration Table

Parameter	Description	Can Entry Be Changed Post-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 Unified Communications Operating System Administration and for logging into the Disaster Recovery System.	Yes, you can change the entry after installation by using the following CLI command: **CLI > utils reset_ui_administrator_name**
Caution Avoid creating administrator account user IDs (for CLI access or OS administration) starting with "uccx" or "UCCX" because such user IDs may conflict with system account names used internally within the Unified CCX server.		
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 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 7 Node Configuration Table

Parameter	Description	Can Entry Be Changed Post-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 Unified CCX.	Yes, you can change the entry after installation by using the following CLI command: **CLI > utils reset_application_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 Unified CCX and Unified CM.	Yes, you can change the entry after installation by using the following CLI command: **CLI > utils reset_application_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) and self-signed certificates.	Yes, you can change the entry after installation by using the following CLI command: **CLI > set web-security**
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, it is important 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 a Unified CCX cluster.	Yes, you can change the entry after installation by using the following CLI command: **CLI > set network dns**

Table 7 Node Configuration Table

Parameter	Description	Can Entry Be Changed Post-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 primary**
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 secondary**
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**
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.	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.	Yes, you can change the entry after installation. For information on how to change the IP Address and Host Name for Unified CCX, see the *Administration Guide Cisco Unified CCX and Cisco Unified IP IVR* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Table 7 Node Configuration Table

Parameter	Description	Can Entry Be Changed Post-Installation
IP Address Your entry:	Enter the IP address of your server.	Yes, you can change the entry after installation. For information on how to change the IP Address and Host Name for Unified CCX, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* or *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
IP Mask Your entry:	Enter the IP subnet mask of this machine.	Yes, you can change the entry after installation by using the following CLI command: **CLI > set network ip eth0**
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. If you are unsure of the MTU setting for your network, use the default value. 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**

Table 7 Node Configuration Table

Parameter	Description	Can Entry Be Changed Post-Installation
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. **Note** You can enter up to five NTP servers.	Yes, you can change the entry after installation by using the following CLI command: **CLI > utils ntp config**
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 while installing the second node to form a cluster.	Yes, you can change the entry after installation by using the following CLI command: **CLI > set password security** To avoid losing communications between nodes, you must change the Security password on both nodes in a cluster and reboot both the nodes. For more information, see the description of this command in the *Cisco Unified Communications Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Table 7 Node Configuration Table

Parameter	Description	Can Entry Be Changed Post-Installation
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**
Organization Your entry:	Enter the name of your organization. **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**
Unit Your entry:	Enter the name of the business unit of your organization. **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**
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 7 Node Configuration Table

Parameter	Description	Can Entry Be Changed Post-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**
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) and self-signed certificates.	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**

Frequently Asked Questions about 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 password, see the "What is a Strong Password?" section on page 26.

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

- Administrator User Name and Password, page 25
- Application User Name and Password, page 25

- Security Password, page 26

Administrator User Name and Password

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

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

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

- Administrator user name—The Administrator user name must start with an alphabetic character and can contain alphanumeric characters, hyphens and underscores.
- Administrator password—The Administrator password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. See the "What is a Strong Password?" section on page 26 for additional information on how to create a strong password.

You can change the Administrator password or add a new Administrator by using the command line interface. For more information, see the *Cisco Unified Communications Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Application User Name and Password

You use the Application User name and password to access applications that are installed on the system, including Cisco Unified Real-Time Monitoring Tool (Unified RTMT).

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. See the "What is a Strong Password?" section on page 26 for additional information on how to create a strong password.

You can change the Application User name and password by using the command line interface. For more information, see the *Cisco Unified Communications Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Security Password

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

The Security password must be at least six characters long and can contain alphanumeric characters, hyphens, and underscores. See the "What is a Strong Password?" section on page 26 for additional information on how to create a strong password.

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 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, such as 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, see the folowing documents:

- *Software and Hardware Compatibility Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html
- Release notes for your product release, available at: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_release_notes_list.html

Can I Install Other Software on the Server?

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

You cannot install or use third-party or Windows-based software applications that you may have been using with a previous version of Unified CCX with Unified CCX 8.0(x).

Using the Unified Communications Answer File Generator

Unified Communications Answer File Generator, a Web application, generates answer files for unattended installations of Unified CCX 8.0(x) or later. Individual answer files (**platformConfig.xml**) are copied to the root directory of a USB key or a floppy diskette and are used in addition to the Unified CCX DVD during the installation process.

The Web application supports the following features:

- Allows simultaneous generation and saving of answer files for unattended installation on the publisher node and the subscriber node.
- Provides syntactical validation of data entries.

- Provides online help and documentation.

However, the Web application supports only basic installations and not upgrades.

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

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

The 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. It is important that you use USB keys that are pre-formatted 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 has been entered. If the installer fails to connect, a relevant message is displayed prompting you 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

Unified CCX 8.0(x) uses a different installation framework than previous releases. The installation process allows you to perform a basic installation, factory installation, installation using Answer File Generator, patch upgrade to a newer service release during the installation, and upgrade from Cisco CRS 5.x and Unified CCX 7.x to Unified CCX 8.0(x).

For a more detailed description of the different installation types, see Table 8.

Table 8 Installation Options

Installtion Type	Description
Basic	This option allows you to install the Unified CCX 8.0(x) software from the installation disc and configure it simultaneously.
Factory	This option allows you to obtain a MCS hardware from Cisco, pre-installed with the Unified CCX 8.0(x) software, which you need to configure upon receiving in order to complete the installation.
Use Answer File Generator	This option allows you to install the Unified CCX 8.0(x) software unattended if you provide the pre-existing configuration information on a USB key or floppy disk.
Apply Patch (upgrade during installation)	This option allows you to apply a patch in order to upgrade the software available on the installation disc. You can only apply one patch during the installation process. **Note** Ensure that you have the upgrade patch available on a DVD or on a remote server prior to choosing this option.

Installing Unified Contact Center Express

This section describes how to install the operating system and Unified CCX 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

For instructions on how to navigate within the installation wizard, see Table 9.

Table 9 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)

Note During installation it is possible for your monitor screen to go blank if you left it unattended for a long time. In such a situation, it is recommended not to use the Space bar as pressing the Space bar chooses the default option available on the current window and moves to the next window.
Instead, press **Escape** on your keyboard to display the current screen with the available options open for you to choose and proceed with the installation.

Starting the Installation

If you are installing the second node to form a cluster, you must configure the host name or IP address of the new node on the first node. From the Cisco Unified CCX Administration Web interface of the first node, choose **System > Server** and enter the IP address or host name of the second node. For more information, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

To start the installation, complete the following steps:

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 pre-installed, 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 Pre-existing Configuration Information" section on page 37.

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**. 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**, click **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:

a. 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**.

b. 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.

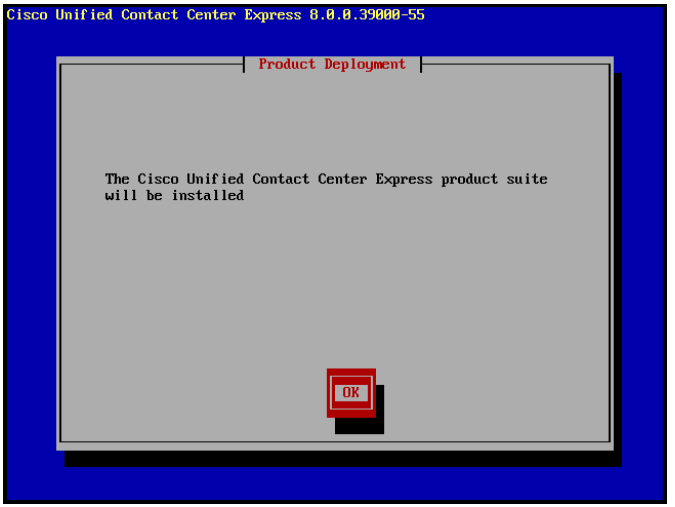
c. The installation process next verifies RAID configuration and BIOS settings.

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

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

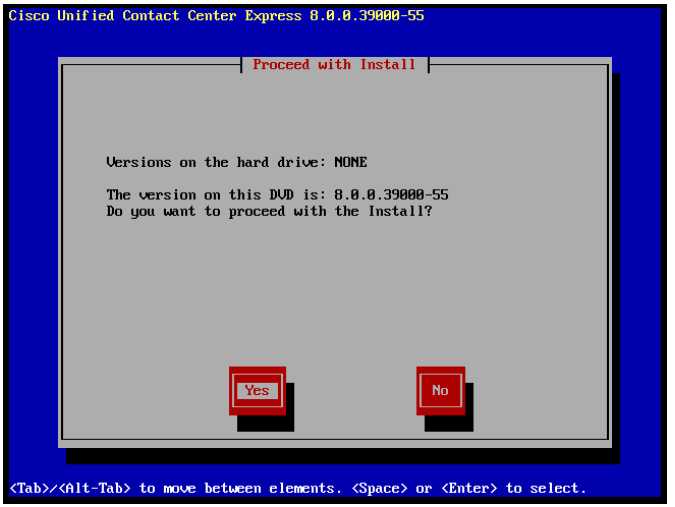
After the hardware check is complete, the Product Deployment window displays (see Figure 1).

Figure 1 Product Deployment Window



Step 6 In the Product Deployment window, click **OK** to install the Unified Contact Center Express product suite. The Proceed with Install window appears (see Figure 2).

Figure 2 Proceed with Install Window



Step 7 If an earlier version of the software is currently installed on the server, the Proceed with Install window displays the software version currently existing on your hard drive and the version available on the DVD. Choose **Yes** to continue with the installation or **No** to cancel.

Caution If you choose **Yes** in the Proceed with Install window, all existing data on your hard drive gets overwritten and lost.

The Platform Installation Wizard window displays (see Figure 3).

Figure 3 Platform Installation Wizard Window

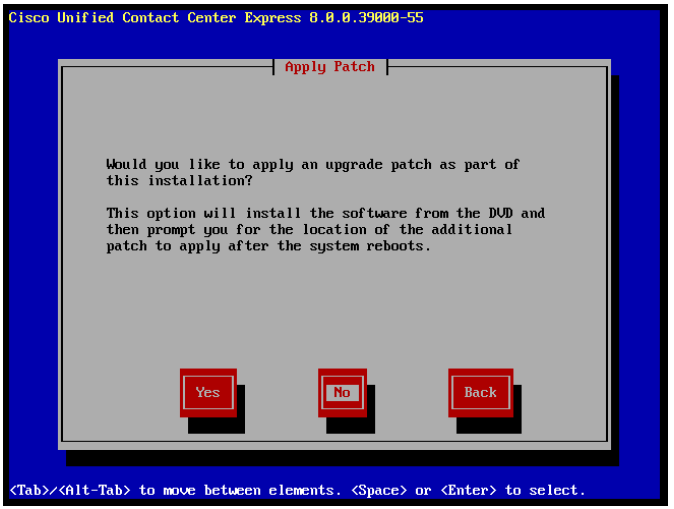
Step 8 Choose one of the following options:

- 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. The Apply Patch window appears (see Figure 4).
- To do any of the following tasks, choose **Skip** and continue with the "Entering Pre-existing Configuration Information" section on page 37.
  - Manually configure the software that is pre-installed on your server—In this case, you do not need to install the software, but you must configure the pre-installed software.

- Perform an unattended installation—In this case, you provide pre-existing configuration information on a USB key, floppy disk or an Answer File Generator.
- 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 pre-install 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 you want to perform, and continue with the following steps. See Table 2 for more information on installation options.

Figure 4 Apply Patch Window



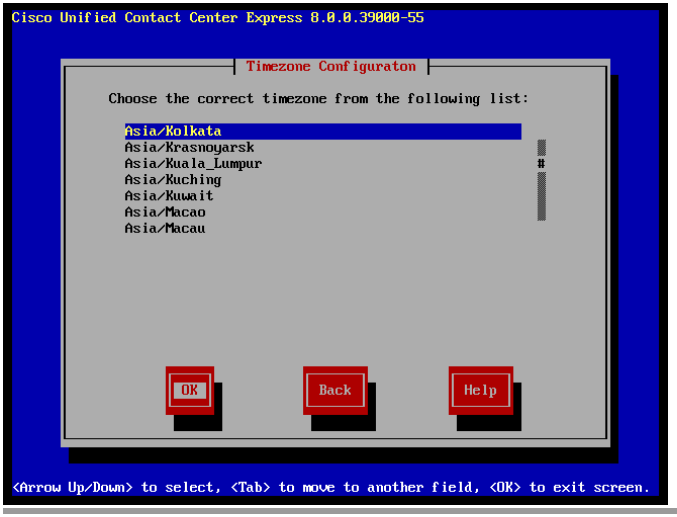
In the Apply Patch window, choose one of the following options:

- To apply a patch and upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the "Applying a Patch" section on page 38.
- To skip this step, choose **No**. The Basic Install window appears (see Figure 5).
- To return to the previous window, choose **Back**.

Figure 5 Basic Install Window

Step 10 In the Basic Install window, choose **Continue** to install the software version on the DVD or configure the pre-installed software. The Timezone Configuration window displays (see Figure 6). Continue with the "Performing the Basic Installation" section on page 42.

Figure 6 Timezone Configuration Window



Entering Pre-existing Configuration Information

Start here if you have a server that has the product pre-installed or if you chose **Skip** in the Platform Installation Wizard window. To start entering pre-existing configuration information, complete the following steps:

Step 1 After the server restarts, the Pre-existing Installation Configuration window displays.

Step 2 If you have pre-existing configuration information created using the Answer File Generator and stored on a CD 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 (see Figure 3).

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

Step 4 Choose the type of installation you want to perform, and continue with the following steps. See Table 8 for more information on installation options.

In the Apply Patch window, choose one of the following options:

- To apply a patch and upgrade to a later Service Release of the software during installation, choose **Yes**. Continue with the "Applying a Patch" section on page 38.
- To skip this step, choose **No**. The Basic Install window appears (see Figure 5).
- To return to the previous window, choose **Back**.

Step 5 In the Basic Install window, choose **Continue**. The Timezone Configuration window displays (see Figure 6). Continue with the "Performing the Basic Installation" section on page 42.

Applying a Patch

If you choose **Yes** in the Apply 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 apply an upgrade patch during installation.

Note You can upgrade to any supported higher release as long as you have a full patch, which is not an engineering special (ES) or a service release (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 *Software and Hardware Compatibility Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_device_support_tables_list.html

You can also find relevant information in the Release Notes for your product release available here:

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/prod_release_notes_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. To start applying the patch, complete the following steps:

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 40.
- **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 40.

- **LOCAL**—Retrieves the upgrade file from a local DVD. Continue with the "Upgrading from a Local Disk" section on page 39.

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.

To start upgrading from a local disk, complete the following steps:

Note Simply copying the ISO file to a DVD will not work.

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

The system installs the patch, then restarts the system with the upgraded software version running. After the system restarts, the Pre-existing Configuration Information window displays.

Step 3 To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays (see Figure 3).

Step 4 To continue the installation, choose **Proceed** or choose **Cancel** to stop the installation.

- If you choose **Proceed**, the Apply Patch window displays (see Figure 4). Continue with Step 5.
- If you choose **Cancel**, the system halts, and you can safely power down the server.

Step 5 When the Apply Patch window appears, choose **No** and continue with "Performing the Basic Installation" section on page 42.

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 to which your server (on which you are applying the patch) has access.

As a selection of SFTP or FTP requires that you configure network settings so that the server can connect to the network, this selection opens with the Auto Negotiation Configuration screen.

To start upgrading from a remote server, complete the following steps:

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 click **OK** to continue.

The MTU Configuration window displays.

Step 4 In the MTU Configuration window, you can change the MTU (maximum transmission unit) size from the operating system default.

The 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 click **OK**.

The Static Network Configuration window displays.

Step 5 For network configuration, enter your static network configuration values and click **OK**. See Table 7 for field descriptions.
The DNS Client Configuration window displays.

Step 6 To enable DNS, choose **Yes**, enter your DNS client information, and click **OK**. See Table 7 for field descriptions.

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

Step 7 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 Validation window displays.

Step 8 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 Pre-existing Configuration Information window appears.

Step 9 To continue the installation, choose **Proceed**.

The Platform Installation Wizard window displays.

Step 10 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 11.

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

Step 11 When the Apply Patch window displays, choose **No** and continue with the "Performing the Basic Installation" section on page 42.

Performing the Basic Installation

To perform the basic installation, complete the following steps:

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

The Auto Negotiation Configuration window displays (see Figure 7).

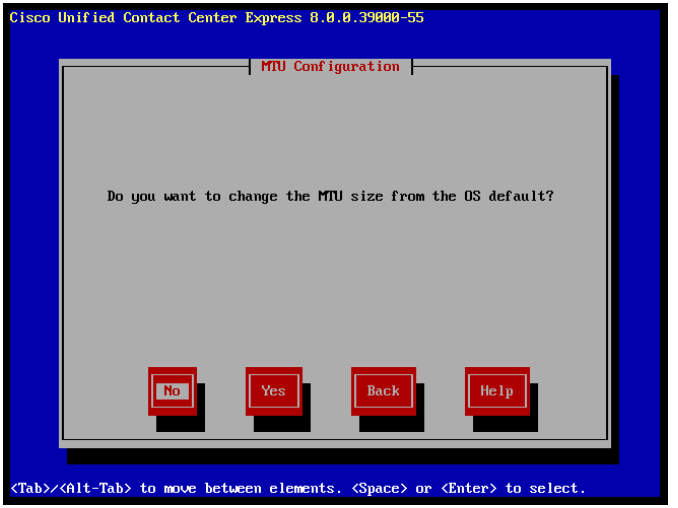
Figure 7 Auto Negotiation Configuration Window

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 (see Figure 8).

Figure 8 MTU Configuration Window



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 click **OK** to continue.

The MTU Configuration window displays (see Figure 8).

Step 4 In the MTU Configuration window, you can change the MTU size from the operating system default.

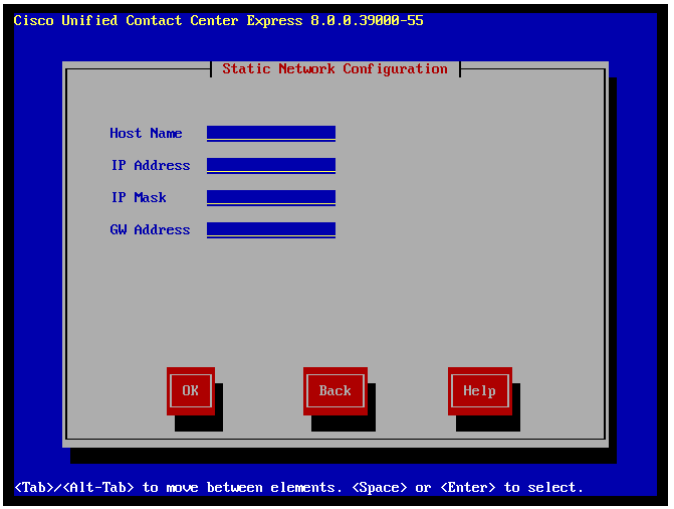
The MTU represents the largest packet, in bytes, that this host will transmit on the network. If you are unsure of the MTU setting for your network, use the default value, which is 1500 bytes.

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 click **OK**.

  The Static Network Configuration window displays (see Figure 9).

Figure 9 Static Network Configuration Window

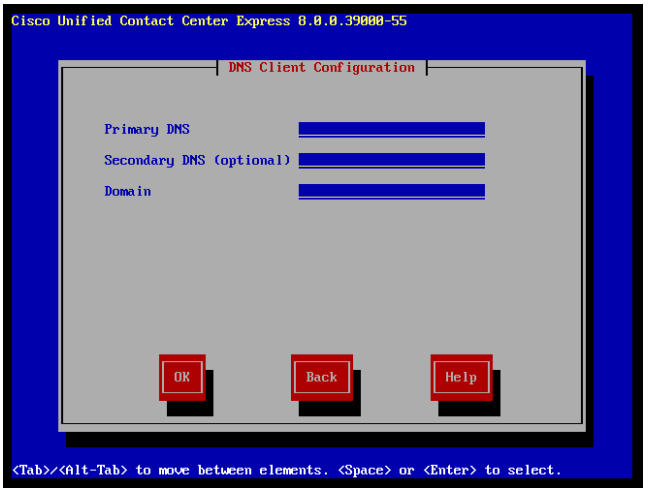


Step 5 For network configuration, enter your static network configuration values and click **OK**. See Table 7 for field descriptions.
The DNS Client Configuration window displays (see Figure 10).

Figure 10 DNS Client Configuration Window - I

Step 6 To enable DNS, choose **Yes**, enter your DNS client information (see Figure 11), and click **OK**. See Table 7 for field descriptions.

Figure 11 Enter Details in the DNS Client Configuration Window



The network restarts by using the new configuration information, and the Administrator Login Configuration window displays (see Figure 12).

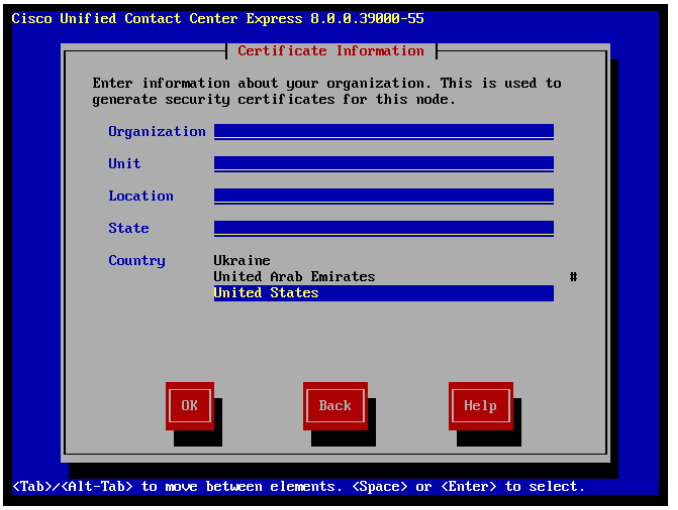
Figure 12 Administrator Login Configuration Window

Step 7 Enter your Administrator login and password from Table 7 and click **OK**. The Certificate Information window displays (see Figure 13).

Note The Administrator ID 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 ID to log in to Unified OS Administration, command line interface, and Disaster Recovery System.

Caution Avoid creating Administrator IDs (for accessing through CLI or for OS administration) starting with "uccx" or "UCCX" because such user IDs may conflict with system account names used internally within the Unified CCX server.

Figure 13 Certificate Information Window



Step 8 Enter data to create your Certificate Signing Request—Organization, Unit, Location, State, and Country and click **OK**.

The First Node Configuration window displays (see Figure 14).

Figure 14 First Node Configuration Window

Step 9 You can configure this server as either the first node or the second node in a Unified CCX cluster.

- To configure this server as the first Unified CCX node, choose **Yes**. The Network Time Protocol Client Configuration window displays (see Figure 15). Continue with the "Configuring the First Node" section on page 49.

Figure 15 Network Time Protocol Client Configuration Window

- To configure this server as the second node in the cluster, choose **No**. The First Node Configuration Warning message displays (see Figure 16). Continue with the "Configuring the Second Node for HA" section on page 57.

Figure 16 First Node Configuration Window with Warning Message

Configuring the First Node

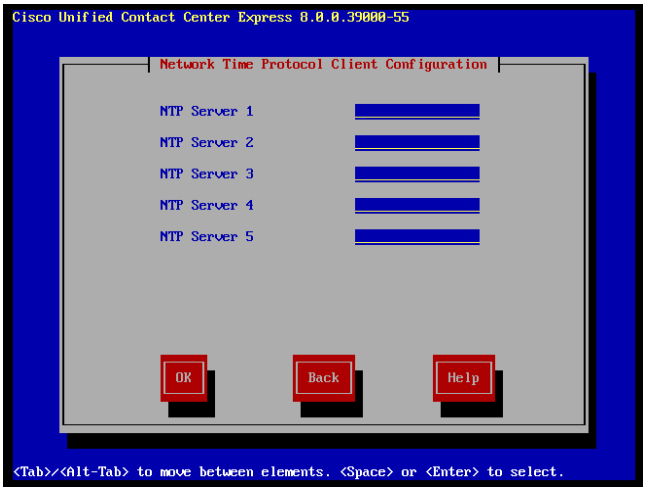
After you finish the basic installation, to configure the server as the first node in the cluster, complete the following steps.

Step 1 In the Network Time Protocol Client Configuration window, choose whether you want to configure an external NTP server or manually configure the system time. If you are installing on a VM image instead of a real server, it is mandatory to use external NTP servers in order to ensure the accuracy of system time.

Note It is important that you use external NTP servers to ensure that system time is kept accurate.

- To set up an external NTP server, choose **Yes** in the Network Time Protocol Client Configuration window (see Figure 16) and then enter the IP address, NTP server name, or NTP server pool name for at least one NTP server (see Figure 17). You can configure up to five NTP servers, and it is important that you use at least three. Click **OK** to continue with the installation.

Figure 17 Setting Up External NTP Servers



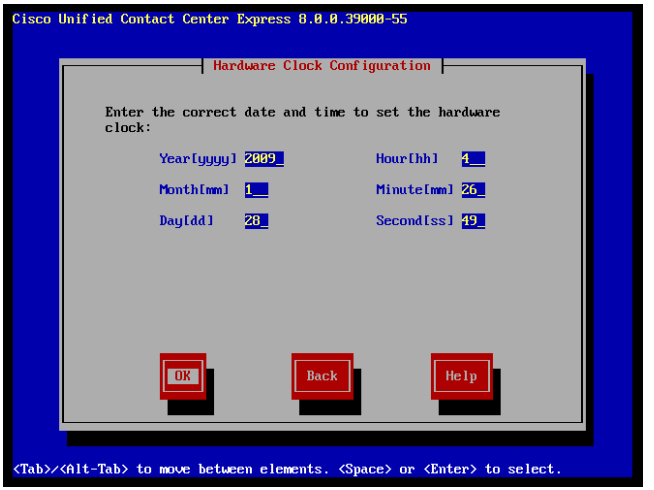
Note Ensure the external NTP server is stratum 9 or higher (meaning stratums 1-9). The second node in a cluster will get its time from the first node.

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, click **No** and enter the appropriate date and time to set the hardware clock in the Hardware Clock Configuration window (see Figure 18).

Figure 18 Hardware Clock Configuration Window



Click **OK** to continue with the installation. The Database Access Security Configuration window displays (see Figure 19).

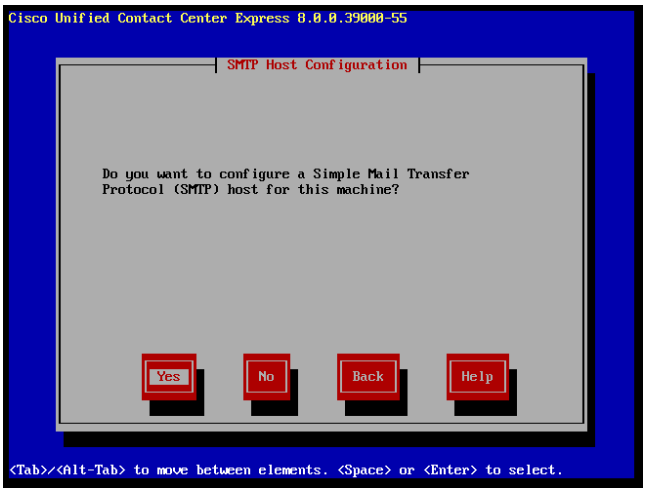
Figure 19 Database Access Security Configuration Window

Step 2 Enter the Security password from Table 7 and click **OK**.

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 both the nodes in a cluster.

The SMTP Host Configuration window displays (see Figure 20).

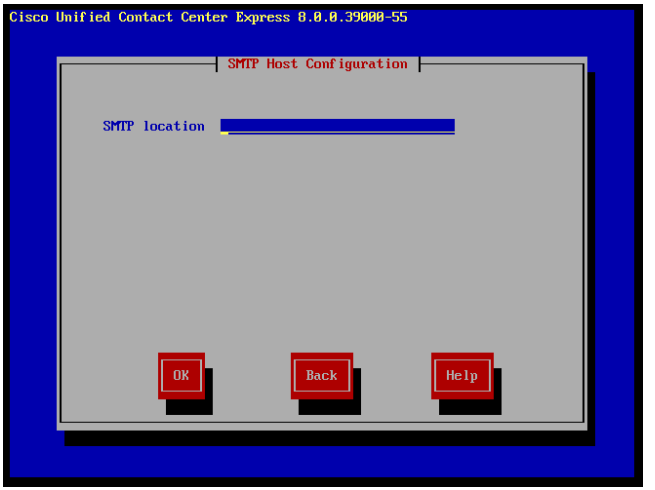
Figure 20 SMTP Host Configuration Window



If you want to configure an SMTP (Simple Mail Transfer Protocol) server for your system, choose **Yes** (see Figure 21).

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.

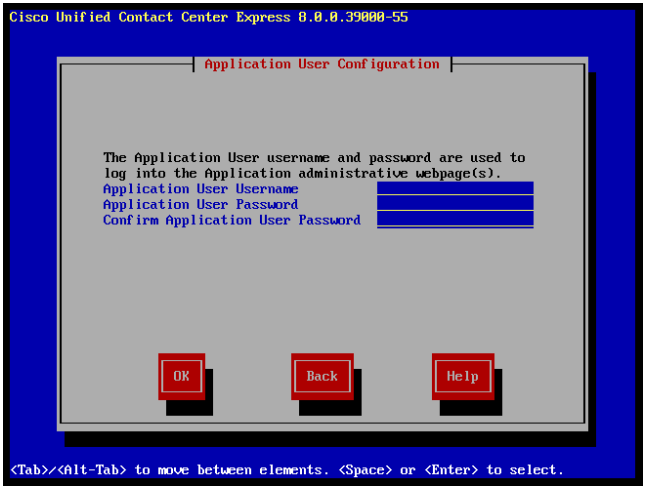
Figure 21 SMTP Host Configuration Window



Step 3 Enter the SMTP host name or IP address in the SMTP Host Configuration window and click **OK**.

The Application User Configuration window displays (see Figure 22).

Figure 22 Application User Configuration Window



Step 4 Enter the Application User name and password from Table 7 and confirm the password by entering it again. Click **OK**.

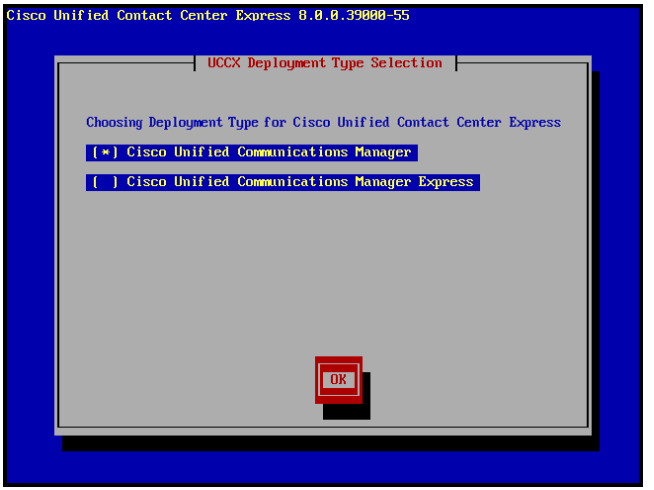
The Platform Configuration Confirmation window displays (see Figure 23).

Figure 23 Platform Configuration Confirmation Window

Step 5 To continue with the installation, click **OK**. The Unified CCX Deployment Type Selection window displays (see Figure 24).

To modify the platform configuration, choose **Back** on the Platform Configuration Confirmation window.

Figure 24 Unified CCX Deployment Type Selection Window



Step 6 In the Unified CCX Deployment Type Selection window, do the following.

a. Choose either of these options:

- **Cisco Unified Communications Manager**—Choose this option if you wish to use Unified CCX with Unified CM
- **Cisco Unified Communications Manager Express**—Choose this option if you wish to use Unified CCX with Unified CME

Note Unified CCX 8.0(x) supports UC500 and UC520 Series Routers. If you deploy Unified CCX 8.0(x) with the UC500 or UC520 Series Routers during installation, select **Cisco Unified Communications Manager Express** as the deployment type in the Unified CCX 8.0(x) installation wizard.

b. Click **OK**.

The system installs and configures the software. The DVD drive ejects, and the server reboots.

Caution Do not reinsert the DVD.

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

Step 8 Complete the post-installation tasks that are listed in the "Performing Post-Installation Tasks" section on page 62.

Adding the Second Node for HA

Before you install Unified CCX 8.0(x) on the second node, you must add the server details of second node on the first node using the Cisco Unified CCX Administration Web interface.

To configure a new server that needs to be added to form a Unified CCX cluster for an HA setup, complete the following steps:

Step 1 On the Cisco Unified CCX Administration Web interface of the first node, choose **System > License Information > Add License(s)**.

Step 2 Browse to select an HA premium or enhanced license and click **Upload**.

Step 3 Once the HA license is successfully uploaded and validated, choose **System > Server**. The List Servers window displays.

You can use the List Servers window to view, add, and remove servers in the cluster.

Step 4 Click **Add New**. The Server Configuration window displays.

Note If you have not uploaded an HA license yet, you will be prompted with a warning message to upload one. Click **OK** to go to the License Information window and upload.

Step 5 In the Server Configuration window, enter the values for the following fields:

Field	Description
Host Name/IP Address	Host name or IP address of the new Unified CCX server to be added to form a cluster. This is a mandatory field.
MAC Address	Physical MAC address of the new server.
Description	Description for the new server.

Note You can add only one additional node. If you have already installed two nodes in the cluster or if you have a Unified CME deployment, the server details of only one node is displayed in this window and the **Add New** button is disabled.

Step 6 Click **Add** to add details of the new server.

Step 7 You can now start installing the second node for HA.

Configuring the Second Node for HA

Once you are done adding the details of second node on the first node using the Cisco Unified CCX Administration Web interface, you can start installing and configuring the second node.

To configure the second node and form a cluster for an HA setup, complete the following steps:

Step 1 If you configured Network Time Protocol (NTP) on the first node, ensure that it is synchronized with an NTP server before you install the second 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 second node will fail.

Step 2 On the First Node Configuration window, read the Warning and make sure you have correctly configured the first node (see Figure 25). To continue with the installation of the second node, click **OK**.

Figure 25 First Node Configuration Warning Window

The Network Connectivity Test Configuration window displays (see Figure 26).

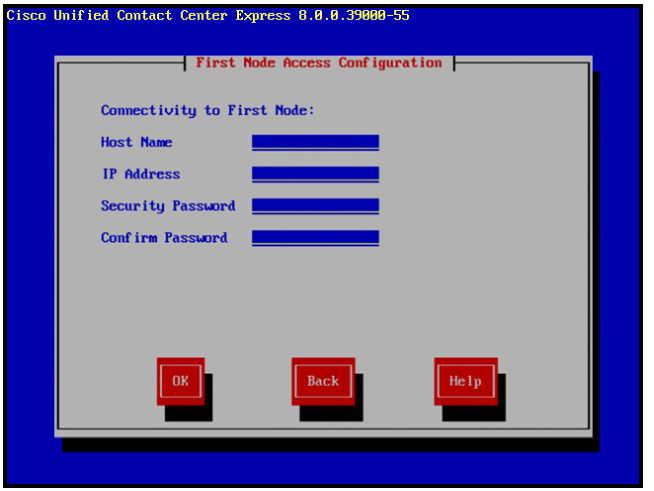
Figure 26 Network Connectivity Test Configuration Window

Step 3 During installation of the second node, the system checks to ensure that the second node can connect to the first node.

- To pause the installation after the system successfully verifies network connectivity, choose **Yes**.
- To continue the installation without a pause, click **No**.

  The First Node Access Configuration window displays (see Figure 27).

Figure 27 First Node Access Configuration Window



Step 4 Enter the first node connectivity information (Host Name, IP Address, and Security Password) and click **OK**.

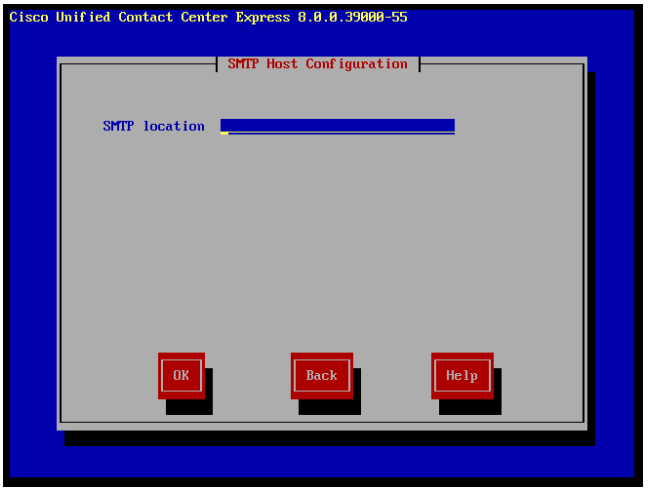
The system checks for network connectivity.

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 re-enter the parameter information.

The SMTP Host Configuration window displays (see Figure 28).

Figure 28 SMTP Host Configuration Window



Step 5 If you want to configure an SMTP server, choose **Yes** and enter the SMTP host name or IP address.

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. If you have configured an SMTP server for the first node, you must configure it for the second node also.

The Platform Configuration Confirmation window displays (see Figure 29).

Figure 29 Platform Configuration Confirmation Window

Step 6 To start installing the software, click **OK**. The system installs and configures the software. The DVD drive ejects, and the system reboots.

Note Your system automatically fetches the configuration information from the first node to set up and configure the second node for HA.

To modify the platform configuration, choose **Back** on the Platform Configuration Confirmation window.

Step 7 When the installation process completes, log in to the Unified CCX Web Administration of the second node using the Application user credentials and complete the post-installation tasks as listed in the "Performing Post-Installation Tasks" section on page 62.

Note Installing the second node and then adding it to the cluster must be done during off peak hours to avoid possible call drops during the formation of a cluster.

Performing Post-Installation Tasks

After installing Unified CCX on your server, you must set some configuration parameters and perform other post-installation tasks before you start using it.

See Table 10 for a list of post-installation tasks.

Table 10 Post-Installation Tasks

Post-Installtion Task	Important Notes
Perform the initial setup for the first node of Unified CCX.	See the "Performing Initial Setup for the First Node" section on page 63 if you have a single node setup.
Perform the initial setup for the second node of Unified CCX.	See "Performing Initial Setup for the Second Node" section on page 73 if you have a two node setup.
The locale English_United_States installs automatically on the server; however, you can add new locales to the server, if required.	See the *Cisco Unified Communications Operating System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
If applicable, configure any network management systems in use at your site.	See the *Cisco Unified Serviceability Administration Guide* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html
Back up your Unified CCX data daily.	See the *Disaster Recovery System Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR* available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Performing Initial Setup for the First Node

After you install Unified CCX, use the Web interface of Cisco Unified CCX Administration to perform the initial system setup.

Cisco Unified CCX Administration is a Web-based application that allows you to control, configure, and monitor many functions of your Unified CCX system. The setup procedure that you perform depends on:

- Your deployment of Unified CCX with Unified CM
- Your deployment of Unified CCX with Unified CME
- Your deployment Unified CCX is SA (single-node) or HA (two-node).

If you later need to update information that you specify during the setup procedure, you can use Cisco Unified CCX Administration to make changes. For more information, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Performing the Initial Setup for a Deployment with Unified CM

After you complete the installation of Unified CCX 8.0(x), you must access the Cisco Unified CCX Administration Web interface through its Authentication page (using the Application username and password that you created during installation) to perform the initial setup procedure.

Start the Initial Setup Configuration on the Unified CCX 8.0(x) Server

To perform the initial setup on the Unified CCX 8.0(x) system, complete the following steps:

Step 1 From any computer in the network that meets the requirements described in the "Client System Requirements" section on page 12, enter the following URL in a Web browser, where *servername* is the host name or the IP address of the server on which you installed Unified CCX and then click the **Cisco Unified Contact Center Express** link.

http://*servername*/

The product information page displays.

Step 2 Click **Cisco Unified Contact Center Express**. The Cisco Unified CCX Administration Authentication window appears.

Note While accessing the Cisco Unified CCX Administration for the first time, a security alert message might appear prompting you to install a security certificate (signed by a third party) if you have not installed a security certificate. This security certficate is required for a secure connection to the server.
For more information on how to install a security certificate, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Step 3 In the Cisco Unified CCX Administration Authentication page, enter the Application username and password that you created during installation (see Table 7).

Note Since the Application user password is case-sensitive, make sure that you enter the password exactly as created.

Step 4 Click **Login**. The Cisco Unified CCX Administrator Setup window for the initial setup procedure displays.

Step 5 Choose **Fresh Install** and then click **Next** to continue.
The Cisco Unified CM Configuration - Service Provider Configuration window displays.

Step 6 In the Cisco Unified CM Configuration - Service Provider Configuration window, enter the **Unified CM hostname or IP address**, **AXL Admin User Name** and **Password** in the respective fields for the Unified CM that you have installed for communicating with Unified CCX 8.0(x), and then click **Next** to continue.
The License Information window displays.

Step 7 In the License Information window, click **Browse** to select the license file that you have purchased, and then click **Next** to continue.
The License Information window with validation information displays.

Step 8 Verify the validation information that appears in the License Information window and then click **Next** to continue.
The Component Activation window displays.

Step 9 Wait until all the components get activated. Once all the components are successfully activated, click **Next** to continue.
The Publisher Activation window displays.

Step 10 Select the checkboxes corresponding to each datastore to activate the Publisher. If the checkboxes corresponding to the listed datastores are already selected and grayed out, it means this is the first node in the cluster which would be the Publisher by default. Click **Next** to continue.
The Cisco Unified CM Configuration window displays.

Step 11 In the Cisco Unified CM Configuration window, the Cisco Unified CCX 8.0(x) AXL Service Provider Configuration area for a Unified CM Cluster setup displays a list of IP addresses of the AXL Service Providers sorted by priority, where the Unified CM Publisher is listed first followed by the Unified CM Subscribers. During the AXL Service Provider Authentication in the Unified CM Cluster deployment, the priority is given to the Unified CM Publisher. However, if the Unified CM Publisher is offline or not available, the next available Unified CM Subscriber is chosen for user authentication. You can also change the priority of the AXL Service Providers, if necessary, by selecting the IP address of an AXL Service Provider in the list and clicking the up and down arrow.

Note As per the Unified CM design, even if the Unified CM Publisher is listed after a Unified CM Subscriber, the system will use the Unified CM Publisher for authentication. However, if the Unified CM Publisher is offline, the Unified CM Subscriber will use its own database to authenticate.

a. In the AXL Service Provider Configuration area, do the following:

- Move the IP address of the Unified CM server or servers that you want to use as the AXL service provider from the **Available AXL Service Providers** list box to the **Selected AXL Service Providers** list box.

  By default, the **Selected AXL Service Providers** list box is pre-populated with the IP address of the server that you specified in Step 5.

  To move an item from one list box to the other, select the item and then click the left arrow (<) or right arrow (>).

- In the **User Name** field, enter a user name for the AXL service provider, if you want to change the name that displays.

This field is pre-populated with the user name that you specified in Step 5.

The AXL Admin user name must not be the Unified CM Administrator username. In case you specify a user name other than the Unified CM Administrator username, add the user name of the AXL Administrator to the Standard Unified CCX Administrators group and "Standard AXL API Access" roles in Unified CM.

- In the **Password** field, enter a password for the AXL service provider, if you want to change the password.

This field is pre-populated with the password that you specified in Step 5.

b. In the Unified CM Telephony Subsystem - Unified CM Telephony Provider Configuration area, do the following:

- Move the IP address of the Unified CM server that you want to use as the Computer Telephony Integration provider for the Unified CM Telephony subsystem from the **Available CTI Managers** list box to the **Selected CTI Managers** list box.

  To move an item from one list box to the other, select the item and then click left arrow (<) or right arrow (>).

- In the **User Prefix** field, enter an application user name for the Unified CM Telephony subsystem.
- In the **Password** and **Confirm Password** fields, enter a password for the Unified CM Telephony subsystem application user.

c. In the RmCm Subsystem - RmCm Provider Configuration area, move the IP address of the Unified CM server that you want to use as the Computer Telephony Integration provider for the RmCm subsystem from the **Available CTI Managers** list box to the **Selected CTI Managers** list box.

To move an item from one list box to the other, select the item and then click left arrow (<) or right arrow (>).

Note Depending on your Unified CCX license, the RmCm Subsystem - RmCm Provider Configuration area may not be available on your system.

d. In the **User ID** field in the RmCm Subsystem - RmCm Provider Configuration area, enter an application user name for the RmCm subsystem.

e. In the **Password** and **Confirm Password** fields in the Unified Telephony Subsystem - Unified CM Telephony Provider Configuration area, enter a password for the RmCm subsystem application user.

Step 12 Click **Next** to continue.
The System Parameters Configuration page displays.

Step 13 In the Systems Parameters Configuration window, do the following:

a. In the **Number of HR Session Licenses** field, enter the maximum number of Unified CCX Historical Reporting sessions that you will run simultaneously.

b. In the **Recording Count** field, enter the maximum number of simultaneous recordings that you will make.

This field displays only if you have a Unified CCX premium license.

c. In the **Number of Outbound seats** field, enter the maximum number of outbound seats.

d. From the **Codec** drop-down list, choose the codec to use for prompts.

Step 14 Click **Next** to continue. The Languages Configuration window displays.

Step 15 In the Languages Configuration window, do the following:

a. In the IVR Language Configuration area, choose a language from the drop-down list that you want to be available for prompts.

A list of available languages for the language group that you selected displays under the **Language Group** column.

b. If you required a custom country-specific language, select the **Group Default** radio button corresponding to that language in order to use it as a base for your custom country-specific language.

c. Check the **Country Specific** check box for each language to install. A country-specific language includes appropriate rules for dates, times, currency, and so on, for the designated country.

d. In the CAD Language Configuration area, choose a language from the **CAD Language** drop-down list that you want to be available for use in the agent desktops and supervisor desktops.

Step 16 Click **Next** to continue. The User Configuration page displays.

Step 17 In the User Configuration page, do the following:

a. In the **Cisco Unified CM Users** list box, select the Unified CM user that you want to designate as the Unified CCX Administrator.

If the desired user does not appear in the **Cisco Unified CM Users** list box, enter part or full user name in the **Search** field and click **Search**.

If you are still unable to find the user in the **Cisco Unified CM Users** list box, you need to create a new user. For more information on how to create a new user in Unified CM, see Creating New Unified CM Users, page 68.

b. Click the left arrow (<) to move the selected user to the **Cisco Unified CCX Administrator** list box.

Step 18 Click **Finish**.
The Cisco Unified CCX Setup Result Information window displays confirming the result of the initial setup. The Unified CCX engine restarts.

Step 19 Close your Web browser.

You have completed the initial setup of Unified CCX. Henceforth, the user selected as the Unified CCX Administrator (in Step 17) can access the Unified CCX Web Administration using the Cisco Unified CCX Administrator credentials.

To change the configuration settings that you made or to perform additional configuration activities, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Creating New Unified CM Users

To create new Unified CM users, follow these steps:

Step 1 Access the Cisco Unified CM Administration Authentication window and log in using the Administrator credentials.

Step 2 In the Cisco Unified CM Administration Setup window, choose **User Management > End User**.

Step 3 In the **Find and List Users** window, click **Add New**.

Step 4 Create an end user by specifying the mandatory fields and other required details.

Step 5 Once the end user creation is successful, navigate back to Cisco Unified CCX Administration and in the User Configuration window, assign the newly created user as **Administrator**.

Step 6 Choose **Tools > User Management** and then select the Administrator Capability View.

Step 7 Click **Update** if the User Configuration window does not display the new end user in the **Cisco Unified CM Users** list box.

Step 8 In the **Cisco Unified CM Users** list box, select the Unified CM user that you want to designate as the Unified CCX Administrator.

Step 9 Click the left arrow (<) to move the selected user to the **Cisco Unified CCX Administrator** list box.

Step 10 Click **Finish**.

Step 11 If the call center needs to be operational after you finish installing the first node, then run the Unified CCX Desktop Client Configuration Tool on this node. You can do so by logging in to the the web interface of the Cisco Unified CCX Administration and then choosing **Tools > Plugin > Desktop suit > Client Configuration Tool**. Let the Unified CCX Desktop Client Configuration Tool run until it stops.

Note If calls are to be taken only after both nodes (in an HA setup) are up, then the Unified CCX Desktop Client Configuration Tool has to run only once, otherwise run it twice; once after the first node is up and one more time after the second node is up.

Performing the Initial Setup for a Deployment with Unified CME

If you are deploying Unified CCX with Unified CME, perform the setup procedure that is described in this section. You perform this procedure one time to provide information about Unified CME, license files, and other system parameters.

To perform the initial setup, complete the following steps:

Step 1 From any computer in the network that meets the requirements described in the "Client System Requirements" section on page 12, enter the following URL in a Web browser, where *servername* is the host name or the IP address of the server on which you installed Unified CCX and then click the **Cisco Unified Contact Center Express** link.

http://*servername*/

The product information page displays.

Step 2 Click **Cisco Unified Contact Center Express**. The Cisco Unified CCX Administration Authentication window appears.

Note While accessing the Cisco Unified CCX Administration for the first time, a security alert message might appear prompting you to install a security certificate (signed by a third party) if you have not installed a security certificate. This security certfication is required for a secure connection to the server. For more information on how to install a security certificate, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Step 3 In the Cisco Unified CCX Administration Authentication page, enter the Application username and password that you created during installation (see Table 7).

Note Since the Application user password is case-sensitive, make sure that you enter the password exactly as created.

Step 4 Click **Login**. The Cisco Unified CCX Administrator Setup window for the initial setup procedure displays.

Step 5 Choose **Fresh Install** and then click **Next** to continue.
The Cisco Unified CME Configuration - AXL User Configuration window displays.

Step 6 In the Cisco Unified CME Configuration - AXL User Configuration window, do the following:

a. In the **Cisco Unified CME server hostname or IP address** field, enter the host name or IP address of the Unified CME router.

b. In the **AXL User ID** field, enter the AXL user ID that you created in Unified CME.

c. In the **AXL User Password** field, enter the AXL password that you created in Unified CME.

Step 7 Click **Next**. to continue.
The License Information window displays.

Step 8 In the License Information window, click **Browse** to select the license file that you have purchased, and then click **Next** to continue.
The License Information window with validation information displays.

Step 9 Verify the validation information that appears in the License Information window and then click **Next** to continue.
The Component Activation window displays.

Step 10 Wait until all the components get activated. Once all the components are successfully activated, click **Next** to continue.
The System Parameters Configuration window displays.

Step 11 In the Systems Parameters Configuration window, do the following:

a. In the **Number of HR Session Licenses** field, enter the maximum number of Unified CCX Historical Reporting sessions that you will run simultaneously.

b. In the **Recording Count** field, enter the maximum number of simultaneous recordings that you will make.

This field displays only if you have a Unified CCX premium license.

Note The **Codec** field does not apply to deployments with Unified CME.

Step 12 Click **Next** to continue. The Languages Configuration window displays.

Step 13 In the Languages Configuration window, do the following:

a. In the IVR Language Configuration area, choose a language from the drop-down list that you want to be available for prompts.

A list of available languages for the language group that you selected displays under the **Language Group** column.

b. If you will create a custom country-specific language, select the **Group Default** radio button corresponding to that language in order to use it as a base for your custom country-specific language.

c. Check the **Country Specific** check box for each language to install. A country-specific language includes appropriate rules for dates, times, currency, and so on, for the designated country.

d. In the CAD Language Configuration area, choose a language from the **CAD Language** drop-down list that you want to be available for use in the agent desktops and supervisor desktops.

Step 14 Click **Next** to continue. The User Configuration page displays.

Step 15 In the User Configuration page, do the following to create login credentials for a new Unified CCX Administrator:

a. In the **User ID** field, enter a user ID for the Unified CCX Administrator.

b. In the **First Name** field, enter the first name of the user. This field is optional.

c. In the **Last Name** field, enter the last name of the user.

d. In the **Name Dialing** field, accept the default entry or enter a new value.

e. In the **Password** Field, enter a password for the user.

f. In the **Confirm Password** field, enter the password again.

g. In the **PIN** field, enter a PIN for the user.

h. In the **Confirm PIN** field, enter the PIN again.

i. Click **Finish**.

The Cisco Unified CCX Setup Result information displays. This window confirms the results of the initial setup.

Step 16 Close your Web browser.

You have completed the initial setup of Unified CCX. Henceforth, the user selected as the Unified CCX Administrator (in Step 15) can access the Cisco Unified CCX Administration using the Administrator credentials.

To change the configuration settings that you made or to perform additional configuration activities, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Performing Initial Setup for the Second Node

Before you install the second node to form a Unified CCX cluster, you should configure the server details for this node on the first node.

To configure a new server that needs to be added to form a Unified CCX cluster for an HA setup, complete the following steps:

Step 1 From any computer in the network that meets the requirements described in the "Client System Requirements" section on page 12, enter the following URL in a Web browser, where *servername* is the host name or the IP address of the server on which you installed Unified CCX and then click the **Cisco Unified Contact Center Express** link.

http://*servername*/

The product information page displays.

Step 2 Click **Cisco Unified Contact Center Express**. The Cisco Unified CCX Administration Authentication window appears.

Note While accessing the Cisco Unified CCX Administration for the first time, a security alert message might appear prompting you to install a security certificate (signed by a third party) if you have not installed a security certificate. This security certficate is required for a secure connection to the server.
For more information on how to install a security certificate, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Step 3 On the Cisco Unified CCX Administration Authentication page, enter the Application username and password that you created during the installation of first node (publisher node).
See step 4 of the "Configuring the First Node" section on page 49 for more information.

Note Since the Application user password is case-sensitive, make sure that you enter the password exactly as created.

Step 4 Click **Login**. The Welcome to Unified CCX Replication Wizard window displays.

Step 5 On the Welcome to Unified CCX Replication Wizard window, enter the following:

Field	Description
Cluster Server IP Address	This field is pre-populated with the first node IP address.
Cisco Unified CCX Administrator User ID	Enter the user name that you created to log in to the first node of Cisco Unified CCX Administration.
Cisco Unified CCX Administrator Password	Enter the password that you created to log in to the first node of Cisco Unified CCX Administration.
Network Deployment Type	Choose the HA network deployment type as either **LAN** or **WAN**.

Step 6 Click **Next**. The Component Activation window displays.

Step 7 Wait until all the components get activated. Once all the components are successfully activated, and then click **Next**.

Step 8 If you have chosen HA network deployment type to be over **LAN**, the Cisco Unified CCX Setup Result Information window displays. This window confirms the result of the setup.

Step 9 If you have chosen HA network deployment type to be over **WAN**, the Cisco Unified CM Configuration window displays.

a. In the Cisco Unified CM Configuration window, enter the configuration parameters for the second node in a similar manner as listed in Step 11 of the "Performing Initial Setup for the First Node" section on page 63.

Note It is important for you to remember that the user credentials for all the three providers/services (listed in Step 11 of the "Performing Initial Setup for the First Node" section on page 63) are cluster-based and valid for both the nodes; therefore, any change made to either of them gets reflected in both the nodes. However, the changes made to the selected Unified CM server for each of the services is specific to that particular node only.

b. Click **Next**. The Cisco Unified CCX Setup Result Information window displays the result of the setup with the warning messages to create CTI port groups (if there are any port groups created in Node 1 prior to adding Node 2, then you need to create the ports for this node) from the CTI Port Group Configuration page and configure individual ASR/TTS servers local to each Unified CCX node so as to make the ASR/TTS feature work over WAN.

c. Perform the tasks as prompted by the warnings before you make your call center operational.

Note It is important that after the Add to Cluser operation is performed, the administrators must configure the failover collector settings for RTMT by choosing **Tools > Service Parameters > AMC Service** in Unified CCX Serviceability.

Step 10 Run the Unified CCX Desktop Client Configuration Tool if you have not run after setting up the first node and then close your web browser.

Note If calls are to be taken only after both nodes (in an HA setup) are up, then the Unified CCX Desktop Client Configuration Tool has to run only once, otherwise run it twice; once after the first node is up and one more time after the second node is up.

You have completed the setting up the Unified CCX second node for HA. To change the configuration settings that you made or to perform additional configuration activities, see the *Administration Guide for Cisco Unified CCX and Cisco Unified IP IVR*, available here: http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Switching Network Deployment from LAN to WAN

You can change a LAN-based two-node setup to work over WAN. To change the network deployment from LAN to WAN for a two-node setup, do the following:

Step 1 Log in to the Publisher node using the Web interface of the Cisco Unified CCX Administration.

Step 2 Choose **System > Server** and delete the Subscriber node (Node 2) from the list.

Step 3 Add the Subscriber node (Node 2) details again on the Publisher node. See "Adding the Second Node for HA" section on page 56 for details.

Step 4 Reinstall Node 2. See "Configuring the Second Node for HA" section on page 57 for details.

Step 5 Choose **WAN** as the **Network Deployment Type** during the initial setup of Node 2. See the "Performing Initial Setup for the Second Node" section on page 73 for details.

Step 6 Add or configure new Unified CM Telephony call control group(s) for the Subscriber node (Node 2).
For more information, see the "*Adding a New Unified CM Telephony Call Control Group*" section of the *Cisco Unified Contact Center Express Administration Guide* available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

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 Unified RTMT. For more information on using and installing the Unified RTMT, see the *Cisco Unified Serviceability Administration Guide*, available here:
http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Obtain Additional Support and Documentation

For information on obtaining support, obtaining additional documentation, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation Feedback

You can provide comments about this document by sending an email to the following address:

ccbu_docfeedback@cisco.com

We appreciate your comments.

Installing Cisco Unified Contact Center Express, Release 8.0(x)