Installation and Upgrade Guide for Cisco Unified Intelligence Center

Release 8.5(3)

December 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0833

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCBs public domain version of the UNIX operating system. All rights reserved. Copyright 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to ***http://www.cisco.com/go/trademarks***

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Copyright 2011 Cisco Systems, Inc. All rights reserved.

Table of Contents

Preface 1
- Purpose 1
- Audience 1
- Organization 1
- Conventions....2
- Obtaining Documentation and Submitting a Service Request....3
- Documentation Feedback....3

1. Before You Install....5
- About Cisco Unified Intelligence Center....5
- Prerequisites and Important Considerations....6
- Completing the Configuration Worksheet....7
- Installation Sequence and Time....8
- Navigating the Installation Wizard....9

2. Preparing to Install Unified IC on a Virtual Machine....11
- Install VMWare ESXi....11
- Deploy the Unified IC Open Virtualization Format/Open Virtual Appliance (OVF/OVA) template on the Virtual Machine....12
- Specify the location of the Unified IC installable....13
- Setting the Boot Order....13
- Install Unified IC on the virtual Machine....14

3. Beginning the Installation - All Nodes....15
- Media and Hardware Check....15
- Basic Install Configuration Information....17

4. Configuring the Controller....21
- Completing the Configuration for the First Node....21

5. Installation....25
- Installation Duration....25
- Installation Processes....25
- Installation Failure....27
- After the Installation....27

6. Sign in to the Administration Console....29
- Upload the License....29
- Define the Member Node in the Administration Console....30
- Verify the Controller is Synchronized with the NTP Server....31

7. Configuring the Member....33
- Begin the Installation and Configuration for the Member Node....33
- Completing the Configuration for the Member Node....33

8. Upgrades and Migrations....35
- About Upgrades....35
- Obtaining the Upgrade File....36
- Accessing Cisco Unified OS Administration....37
- Upgrading from DVD/CD 38
- Upgrading from Remote Filesystem....39
- Reverting to a Previous Version....40

About Migrations....41
Backing up data from the Cisco Unified IC Release 8.0(3)....41
Installing Cisco Unified IC Release 8.0(3) over a Virtual Machine....42
Restoring the backed up data on the Cisco Unified IC Virtual Machine....42
9. Frequently Asked Questions about the Installation....45
Can I Install on a Virtual Machine?....45
Can My Cisco Support Provider Log In to Assist Me?....46
Error Message about "No Such File or Directory"....46
How Do I Access Log Files?....46
How Do I Add or Replace a Device in the Cluster?....47
How Do I Find the Server MAC Address?....47
How Do I Sign In to the Administration Console?....47
How Do I Sign In to Unified IC Reporting?....48
How Do I Switch Between the Administration Console and Unified IC Reporting?....48
How Do I Access the Command Line Interface?....48
How Do I Test Server Connectivity? 49
How Do I Use the Recovery Disk?....49
How Do I Uninstall?....49
How is Data Handled During an Upgrade? 50
Is Unified IC Supported in a Hosted Deployment?....50
Unified IC Licenses....50
How To Obtain Your License....51
How to Upload the License....52
License Types....52
Feature Set for Standard and Premium Licenses....52
What Accounts and Passwords are Defined During the Installation?....53
What if the Installation Fails?....55
How to Dump Install Logs to the Serial Port of the Virtual Machine....55
What To Do if the Upgrade Stalls....56
Where is a Fresh Installation Installed?....56
Where is an Upgrade Installation Installed?....56
Index 59

List of Figures

Figure 1: Virtual Machine Install Screen....23
Figure 2: License Screen....26
Figure 3: Cryptographic Screen....27
Figure 4: Device Configuration....30
Figure 5: Member Configured....31
Figure 6: Unified OS Administration....37
Figure 7: Software Upgrade page....38
Figure 8: Installation Failed Screen....55

Preface

Purpose

This guide explains how to install Cisco Unified Intelligence Center (CUIC) Release 8.5(3).

Audience

This guide is prepared for partners, specialists, and system administrators who are responsible for the installation of Unified IC.

Note: This document might not represent the latest Cisco product information available. Obtain the most current documentation at this URL: **http://www.cisco.com/en/US/products/ps9755/tsd_products_support_series_home.html** .

Organization

In addition to this preface, this guide is arranged as follows:

This Chapter	Covers
Chapter 1, Before You Install (page 5)	An overview of the Unified IC A configuration worksheet for gathering information needed for the installation
Chapter 2, Beginning the Installation - All Nodes (page 11)	The media check and the hardware check The basic configuration screens for all nodes

This Chapter	Covers
Chapter 3, Configuring the Controller (page 21)	Configuration steps for the Controller node
Chapter 4 - Installation (page 25)	Processes that occur during the installation.
Chapter 5, Sign in to the Administration Console (page 29)	Signing in to the Administration interface to upload the license and create the Member information
Chapter 6 - Configuring the Member(s) (page 33)	Configuration steps for the Member node
Chapter 7 - Software Upgrades (page 35)	Explains how to use Cisco Unified OS Administration to upgrade your Unified IC software
Chapter 8 - Frequently Asked Questions about the Installation (page 45)	Tips and frequently-asked questions

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example: • Choose **Edit** > **Find**. • Click **Finish**.
italic font	Italic font is used to indicate the following: • To introduce a new term. Example: A *skill group* is a collection of agents who share similar skills. • For emphasis. Example: *Do not* use the numerical naming convention. • A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*) • A book title. Example: See the *Cisco CRS Installation Guide*.
`window font`	Window font, such as Courier, is used for the following: • Text as it appears in code or that the window displays. Example: `<html><title>Cisco Systems,Inc. </title></html>`

Convention	Description
< >	Angle brackets are used to indicate the following: • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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 email to the following address:

mailto:ccbu_docfeedback@cisco.com

We appreciate your comments.

Documentation Feedback

Chapter 1

Before You Install

This chapter contains the following topics:

- About Cisco Unified Intelligence Center, page 5
- Prerequisites and Important Considerations, page 6
- Completing the Configuration Worksheet, page 7
- Installation Sequence and Time, page 8
- Navigating the Installation Wizard, page 9

About Cisco Unified Intelligence Center

Unified IC can be installed as a standalone server or as a cluster of a maximum of eight server nodes. There is one mandatory publisher node (called the *Controller*) and a maximum of seven subscriber nodes (called *Members*). The Controller node includes a Member; thus a deployment can consist of a Controller only.

All nodes must meet latency requirements as described in the SRND.

The primary node (the *Controller*) includes both the Administration (Operations, Administration, Maintenance, and Provisioning or OAMP) and the Unified IC Reporting web applications. A Controller is required in all deployments. A deployment can consist of a Controller only.

The Member nodes have the Unified IC Reporting web application only.

Unified IC is installed on Cisco Unified Voice Operating System (VOS). This is an appliance model or "closed box" and does not support navigation into, or manipulation of, the file system.

Unified IC must be installed on Multimedia Communications Servers (MCS) or equivalent hardware, or a Virtual Machine running over UCS B-Series and C-Series Servers.

The disk capacity and hardware type of Member nodes should be equal to or greater than those of the Controller node.

Refer to the **Cisco Unified Intelligence Center Hardware and System Software Specification (Bill of Materials)** (http://www.cisco.com/en/US/products/ps9755/products_implementation_design_guides_list.html) for server requirements and version compatibility.

Refer to the Cisco Unified Intelligence Center Solution Reference Network Design (SRND) Guide, available at in the Design Guides category at **http://www.cisco.com/en/US/products/ps9755/tsd_products_support_series_home.html**

Prerequisites and Important Considerations

Before you proceed with the installation, upgrade, or migration, note these requirements and recommendations:

- You must have access to a Network Time Protocol (NTP) server.
- You must have a preconfigured default router.
- You must have a preconfiigured Domain Name Server (DNS).
- You must install the primary node (the Controller) first.
- Request a license file from Cisco Systems, Inc. See How to Obtain Your License (page 51). When the primary node installation is complete, and *before installing* a Member node, you must sign in to the Administration console to apply the license and to define the Member node.
- When you are migrating from the traditional MCS servers to a Virtual Machine-based UCS server, you typically perform a backup from the old server and restore the data on the new server. The backed up license does not work on a Virtual Machine. You need to get a different license for the Virtual Machine based on the licensing MAC. See How to Obtain Your License (page 51).
- When you are migrating from the traditional MCS servers to a virtual server, ensure that the new Virtual Machine instance have the same hostname and IP address as that of the machine from which you are migrating.
- All configured nodes in a cluster must be installed and started before you install a new node. For example, if the Controller and one Member have been installed and you are about to add a second Member, the Controller and first Member must be started and available so that the second Member is able to access them.
- Installation on an existing (repurposed) server formats the hard drive and erases all data. It might also change the system Basic Input Output System (BIOS), firmware, and Redundant Array of Inexpensive Disks (RAID) configuration.
- On the installation configuration screens:
  - Many values—such as host names, User IDs, and passwords—are case-sensitive.

– You must enter the same security password on all nodes in the cluster. Keep a record of this password; you will need to use it if you replace or add a server in the future or if you want to replace the old secutiry password with a new one.

– Use the default Maximum Transmission Unit (MTU) setting, which is 1500, for all nodes in the cluster.

Completing the Configuration Worksheet

Use this worksheet to record network and password information that the basic installation configuration wizard prompts you to enter. Store this worksheet information for future reference.

Table 1: Configuration Worksheet

Configuration Data	Your Entry
Host Name	Controller _____ Member 1 _____ Member 2 _____
IP Address	Controller _____ Member _____
Gateway (GW) Address	_____
Primary DNS IP Address	Controller _____ Member _____
Secondary DNS IP Address	Controller _____ Member _____
Domain	_____
System Administrator (page 53) Username **Note:** As a best practice, use the same System Administrator credentials for all nodes.	_____
System Administrator Password	_____
Timezone Use the same Timezone for all nodes.	_____
Certificate Information	Organization:_____ Unit:_____

Configuration Data	Your Entry
	Location:_____ State:_____ Country:_____
NTP Server Host Name or IP Address	NTP Server 1: _____ NTP Server 2: _____ NTP Server 3: _____ NTP Server 4: _____ NTP Server 5: _____
Database Access Security Password Servers in the cluster use the security password to communicate with one another. The security password is also used by the Disaster Recovery System (DRS) for encryption of the backup file. **Note:** You must enter the same security password for all servers in the cluster.	Security Password: _____
Simple Mail Transfer Protocol (SMTP) Location Host Name	SMTP Host Name or IP Address: _____
System Application User (page 54) Credentials **Note:** As a best practice, use the same System Application credentials for all nodes. The Application User defined during the Controller installation is the only credential recognized by Unified IC.	Application User ID: _____ Application User Password: _____

Installation Sequence and Time

A Unified IC can include one or multiple nodes. The installation for each node can take about an hour. For most of that time, it can run unattended.

You must perform the installation on the primary node/Controller first.

Some configuration and installation processes differ slightly for the first node (Controller) and for the Members. This is noted in these instructions.

Navigating the Installation Wizard

Much of the installation requires no action on the part of the person who runs it. When user input *is* required, use the following *keyboard* navigation and selection actions.

The installation wizard screens do not recognize a mouse or a touchpad.

Table 2: Installation Wizard Navigation

To Do This	Press This Key
Move to the next field	Tab
Move to the previous field	Alt-Tab
Choose an option	Spacebar
Scroll up or down a list	Up or Down arrow keys
Go to the previous screen	Tab to Back and press the Spacebar
Get information on a screen	Tab to Help and press the Spacebar
Scroll up and down a list	Up or Down arrow keys

Chapter 2

Preparing to Install Unified IC on a Virtual Machine

Starting with Release 8.0(3), you can either perform a fresh installation of Cisco Unified Intelligence Center Release 8.0(3) or migrate from a previous release of Cisco Unified Intelligence Center Release 8.0(1) or 8.0(2) to Release 8.0(3) on a UCS B-Series or C-Series Server (Virtual Machines).

The initial steps for both scenarios are common. Wherever there is a change, it is noted as such in this document.

To know more about the Unified Communications Virtualization, refer to **Unified Communication Virtualization** (http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization)

This chapter contains the following topics:

- Install VMWare ESXi, page 11
- Deploy the Unified IC Open Virtualization Format/Open Virtual Appliance (OVF/OVA) template on the Virtual Machine, page 12
- Specify the location of the Unified IC installable, page 13
- Setting the Boot Order, page 13
- Install Unified IC on the virtual Machine, page 14

Install VMWare ESXi

Before you begin your Unified IC installation, you must install VMware ESXi and configure the virtual server.

Step 1 Refer to **Unified Communication Virtualization** (http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization) to install, setup, and configure the UCS Hardware.

Step 2 Configure the UCS Network. Refer to **UCS Network Configuration** (http://docwiki.cisco.com/wiki/Unified_Contact_Center_Enterprise#UCS_Network_Configuration).

Step 3 Use the instructions mentioned in the appropriate server documentation to install VMWare ESXi on your UCS server:

a. To install ESXi on a **UCS B-series server**, refer to **Cisco UCS B-Series Servers VMware Installation Guide** (http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/b/os/vmware/install/bseries-vmware-install.html)

b. To install ESXi on a **UCS C-series server**, refer to **Cisco UCS C-Series Servers VMware Installation Guide** (http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/os/vmware/install/vmware_install_c.html)

Step 4 After ESXi is installed successfully, reboot the server.

Deploy the Unified IC Open Virtualization Format/Open Virtual Appliance (OVF/OVA) template on the Virtual Machine

Open Virtualization Format/Open Virtual Appliance (OVF/OVA) is an open standard for packaging and distributing virtual appliances. Files in this format have an extension of .ova. The naming convention for the OVF/OVA template is **`PRODUCT_COMPONENT_USER COUNT_VERSION_VMVER.ova`**.

The OVF/OVA template defines the configuration of the virtual machine hardware. The configuration of a Cisco Unified Communications application virtual machine must match a supported virtual machine template. This section describes the steps to deploy a Unified IC OVF/OVA template on the virtual machine.

Step 1 Login to **ESXi** using *VMWare Vsphere* or any other compatible client

Step 2 Highlight the host or cluster to which you want to deploy the Virtual Machine.

Step 3 Select **File > Deploy OVF/OVA Template**.

Step 4 Click **Deploy from File** and specify the name and location of the OVF/OVA file (with a *.ova* extension)

Alternatively, you can click **Deploy from URL** and specify the URL of the OVF/OVA file.

Step 5 Click **Next**.

Step 6 Verify the details of the template, and click **Next**.

Step 7 Specify a name for the **Virtual Machine** that you are about to create and choose an inventory location on your host.

Step 8 Click **Next**.

Step 9 Verify the deployment settings, and click **Finish**.

The virtual machine that you added is listed under the UCS server tree in the **vSphere Client** home page.

Specify the location of the Unified IC installable

Step 1 Select the newly added Virtual Machine.

Step 2 From the **Inventory** menu, select **Virtual Machine** > **Edit Settings**.

Step 3 In the **Hardware** tab, select **CD/DVD Drive 1**.

Step 4 Select one of the following option to specify the location where you have the bootable Unified IC installer file:

a. **Client Device** – If you want to use the CD/DVD drive on the client machine from where you are accessing the virtual machine remotely.

b. **Host Device** – If you want to use the CD/DVD drive on the ESXi host machine.

c. **Datastore ISO file** – If you want to use the datastore on the virtual machine. Before using this option, ensure that the Bootable iso image of Unified IC is copied to the datastore of the ESXi host.

Note: Cisco recommends you to set the boot order by making **CD ROM** as the first device upon power up. For details, refer Setting the Boot Order (page 13).

Step 5 Click **OK** to save and close the **Virtual Machine Properties** window.

Important: Make sure that you have copied or inserted the CD/DVD with the Unified IC installable in the appropriate location before you proceed with the next step.

Setting the Boot Order

To set the boot order:

Step 1 From the **Inventory** menu, select **Virtual Machine** > **Edit Settings**.

The Virtual Machine Properties window appears.

Step 2 In the **Options** tab, select **Boot Options**.

Step 3 Select **Force BIOS Setup**.

Note: When you restart the Virtual Machine, you will see the BIOS screen in the **VM console** tab.

Step 4 In the **BIOS** screen, select **Boot Options** > **make the CD/DVD ROM as the first device for bootup**.

Step 5 Click **Save**.

Install Unified IC on the virtual Machine

Step 1 Select the virtual machine and click **Power** > **Power On** from the shortcut menu. Alternatively, from the **Inventory** menu, select **Power** > **Power On**.

Step 2 The virtual machine powers on and Unified IC installation starts up automatically. Follow the steps mentioned in Beginning the Installation (page 15) to complete the Unified IC installation.

Note: vSphere provides you with a console that you can use to provide inputs during the installation. To open the console, select the virtual machine from the vSphere home page and click **Open Console** from the shortcut menu. Alternatively, select the virtual machine and click the **Console** tab in the right pane of the **vSphere** home page. Pointing and clicking anywhere in the console window will allow you to enter data in the console. Once you start working on the console, the mouse is locked and you can no longer use it. Use **Tab** key to navigate and use the **Enter** button to commit the values you entered. To release the mouse from the console window, press **Ctrl + Alt**.

Chapter 3

Beginning the Installation - All Nodes

The installation for Unified IC is delivered on DVD media. Run the DVD installation on each node and use the *same* DVD for all nodes.

Note: All nodes in a must be running the same version of Unified IC.

This chapter contains the following topics:

- Media and Hardware Check, page 15
- Basic Install Configuration Information, page 17

Media and Hardware Check

Every installation begins with an optional pre-install media check and includes a hardware check.

Step 1 Insert the installation DVD into the tray. Then restart or power on the server so that it boots from the DVD.

You see messages as the pre-install script runs. When the pre-install script ends, the DVD Found screen opens.

Step 2 In the **DVD Found** screen, you have the option to perform a media check to verify the integrity of the DVD.

If	Then
You want to check the media. **NOTE that** the media check can take up to an hour. If the media check for the Controller passes, you	Select **Yes** to begin the verification of the media integrity. If the media check passes, select **OK**. Continue to Step 3.

If	Then
can safely skip the media check when you install the Members.	If the media check fails, the DVD is ejected and the installation terminates. Contact your support provider for assistance.
You want to skip the media check.	Select **No**. A message displays at the bottom of the monitor: *Running the Cisco Unified Communications 8.0 system installer. Please Wait...* Then the Product Deployment Selection screen opens. Proceed to Step 3.

Step 3 The **Product Deployment Selection** screen states that the Cisco Unified Intelligence Center product will be installed. This screen has only one choice—**OK**. Select **OK** to open the Proceed with Install screen.

Clicking OK initiates a check for hard drive sanity, during which the installation checks for a supported hardware platform with the correct number of disks.

A successful hardware check opens the Proceed with Install screen.

Note: If the server hardware is unsupported, a message is displayed indicating that the installation cannot proceed, and the installation halts. If you require assistance understanding the message, write it down to facilitate your conversation with your support provider. Refer to the **Cisco Unified Intelligence Center Bill of Materials** (http://www.cisco.com/en/US/products/ps9755/products_implementation_design_guides_list.html) for details on supported hardware.

Step 4 The **Proceed with Install** screen shows the version of the product that is currently on the hard drive (if any) and the version of the product that is on the DVD. For the initial installation, the version on the hard drive shows NONE.

Select **Yes** at the Proceed with Install screen to open the Platform Installation Wizard screen.

Step 5 In the **Platform Installation Wizard** screen, select **Proceed** to open the Apply Patch screen.

Step 6 Select **No** at the Apply Patch screen. You do not apply patches from the Installation wizard. Refer to Chapter 7 - Software Upgrades (page 35) for instructions on upgrading Unified IC software with Engineering Specials, Minor Releases, and Maintenance Releases.

Your selection of No opens the Basic Install screen.

Note: If you select Yes by mistake and open the Apply Patch screen, select **Back.**

Step 7 Select **Continue** at the Basic Install screen to enter the configuration screens.

Basic Install Configuration Information

The Basic Install launches a series of screens that present questions and options pertinent to the platform and the setup configuration. There is online help for each wizard screen.

Note: You can change many of the basic installation configuration settings after the installation using the Set commands in the Command Line Interface (CLI). The CLI is documented in the *Administration Console User Guide for Cisco Unified Intelligence Center*.

The first Basic Install wizard screen is Timezone Configuration.

Step 1 In the **Timezone Configuration** screen:

a. Use the down arrow to select the local timezone that most closely matches where your server is located. You can also type the initial character of the timezone to move to that item in the list. The timezone field is based on country/city and is mandatory. Setting it incorrectly can affect system operation.

Note: Use the same timezone for all nodes.

b. Select **OK** to open the Auto Negotiation Configuration screen.

Step 2 In the **Auto Negotiation Configuration** screen, select whether or not you want to use automatic negotiation for the settings of the Ethernet network interface card (NIC).

If	Then
You want to disable auto-negotiation and specify NIC speed and duplex settings.	Select **No** to open the NIC Speed and Duplex Configuration screen, where you can manually configure the settings. Proceed to Step 3.
The ethernet network interface card (NIC) attached to your hub or Ethernet switch supports automatic negotiation.	Select **Yes** to open the MTU Configuration screen. Proceed to Step 4.

Step 3 In the **NIC Speed and Duplex Configuration** screen, configure settings as follows:

a. Specify the speed of the Network Interface (NIC) card in megabits per second. Speed options are **10** or **100**.

b. Specify the duplex setting of the server NIC. Options are **Full** or **Half**.

c. Select **OK** to open the MTU Configuration screen.

Step 4 In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units (1500). If you do not accept the default and configure the MTU size incorrectly, your network performance can be affected.

Your selection of No opens the DHCP Configuration screen.

Step 5 In the **DHCP Configuration** screen, select **No** to open the Static Network Configuration screen.

Step 6 At the **Static Network Configuration** screen, enter static network configuration values as follows, referring to the Configuration Worksheet (page 7) if necessary:

a. Enter the **Hostname**.

b. Enter the **IP Address**.

c. Enter the **IP Mask**.

d. Enter the **GW Address**,

e. Select **OK** to open the Domain Name System (DNS) Client Configuration screen.

Step 7 Enter your DNS client information as follows, referring to the Configuration Worksheet (page 7) if necessary:

a. Enter the **Primary DNS** (mandatory).

b. Enter the **Secondary DNS** (optional).

c. Enter the **Domain** (mandatory).

d. Select **OK** to open the Administrator Login Configuration screen.

Step 8 In the **Administrator Login Configuration** screen:

a. Enter the ID for the System Administrator. See the FAQ on Accounts and Passwords (page 53) for the permissions and responsibilities of this administrator.

b. Enter and then confirm the password for the administrator.

c. Select **OK** to open the Certificate Information screen.

Step 9 In the **Certificate Information** screen:

a. Enter data to create your Certificate Signing Request—Organization, Unit, Location, State, and Country.

b. Select **OK** to open the First Node Configuration screen. ("Is this the First Node in the cluster?")

Step 10 In the **First Node Configuration** screen, specify whether you are configuring the first node (the Controller).

If	Then
You are installing and configuring the primary node (the Controller).	Select **Yes** to open the Network Time Protocol Client Configuration screen.

If	Then
	Continue to Step 1 in Chapter 3 (page 21).
You are installing and configuring a secondary node (a Unified IC Member).	Select **No** to open the First Node Configuration Warning screen. Continue to Completing the Configuration for the Member Node (page 33).

Chapter 4

Configuring the Controller

Completing the Configuration for the First Node

When you complete the basic install configuration and select **Yes** to indicate that you are installing the first node, perform the following steps to complete the configuration for the Controller.

The first screen you see is the **Network Time Protocol Client Configuration** screen.

This screen gives the option of setting the time for the first node (the Controller) from a time that you set on the Hardware Clock screen - or - from an external Network Time Protocol server that you define.

NTP server configuration is mandatory for Unified IC installation over a Virtual Machine.

Note: Network Time Protocol configuration is set for the first node. Other nodes set their time to the time on the first node.

Step 1 Select **Yes** at the **Network Time Protocol Client Configuration** screen.

The **Network Time Protocol Client Configuration** screen opens.

Step 2 Enter the IP address, NTP server name, or NTP Server Pool name for at least one external NTP server.

You can add up to five NTP servers and make changes to the NTP server list at a later time.

Note: Cisco recommends that you use a minimum of three external NTP servers. If you install the first node over MCS server, an option to skip NTP server configuration is available.

Step 3 When you complete the NTP configuration, select **OK**.

The Security Configuration screen opens.

Step 4 In the **Security Configuration** screen:

a. Enter the Database Access Security password. This is the password that servers in the cluster use to communicate with each another. *You must enter the same security password for all servers.*

b. Select **OK** to open the SMTP Host Configuration screen.

Step 5 In the **SMTP Host Configuration** screen, select whether you want to configure an SMTP host to receive platform-level emails; for example, emails about certificate expiration. This field is optional. You will configure email for report scheduling in the Administration console.

If	Then
You want to configure an SMTP Host.	Select **Yes** to open the second SMTP screen opens. Proceed to Step 6.
You do not want to configure an SMTP Host.	Select **No** to open the Application User Configuration screen. Proceed to Step 7.

Step 6 In the second **SMTP Host Configuration** screen:

a. Enter the hostname or IP address for the SMTP server.

b. Select **OK** to open the Application User Configuration screen.

Step 7 Complete the **Application User Configuration** screen. The application user for the Controller becomes the System Application User and the default Super User. See the FAQ on Accounts and Passwords (page 53) for the permissions and responsibilities of the System Application User.

Note: Although it is possible to enter unique Application User credentials on each installed node, it is a best practice to enter the *same* Application User Name and password on all nodes. The Application User credentials entered during the Controller installation are the only ones recognized by Unified IC.

a. Enter the application username.

b. Enter and confirm the application user password.

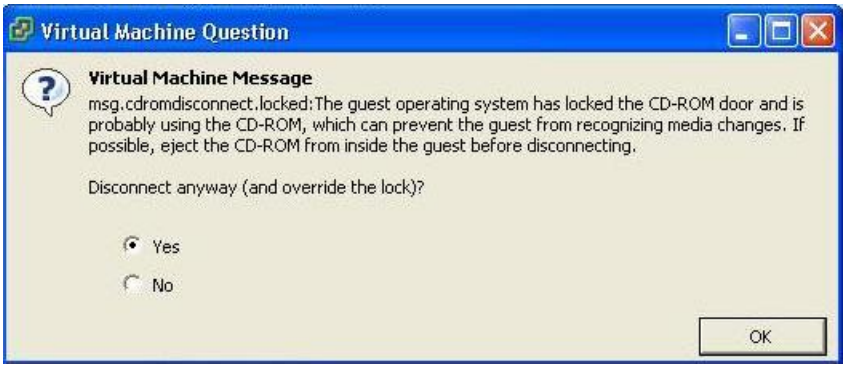
c. Select **OK** to open the Platform Configuration Confirmation screen. This screen states that the platform configuration is complete.

Step 8 In the **Platform Configuration Confirmation** screen, select **OK**.

Step 9 The Installation (page 25) begins.

Note: If installing over a Virtual Machine, the system will display the following screen:

Figure 1: Virtual Machine Install Screen



Select **Yes** and click **OK** to continue installation. The system displays the following message: *The system will reboot momentarily to continue with the installation.*

After the reboot, the system will automatically proceed with the installation.

Chapter 5

Installation

Installation Duration

The installation can take from 60 to 75 minutes to complete and can run unattended for most of that time.

Installation Processes

During the installation, the monitor shows a series of processes, as follows:

- Formatting Progress Bars
- Copying File Progress Bar
- Platform Installation Progress Bars (as multiple packages are installed)
- Post Install Progress Bar
- Application Installation Progress Bars (multiple packages are backed up to the archive directory)
- An informational screen saying that the system will reboot.

  Note: At the start of the reboot, the CD tray holding the DVD ejects. This is normal. You can remove the DVD.

- A System Reboot, which includes a second hardware check.

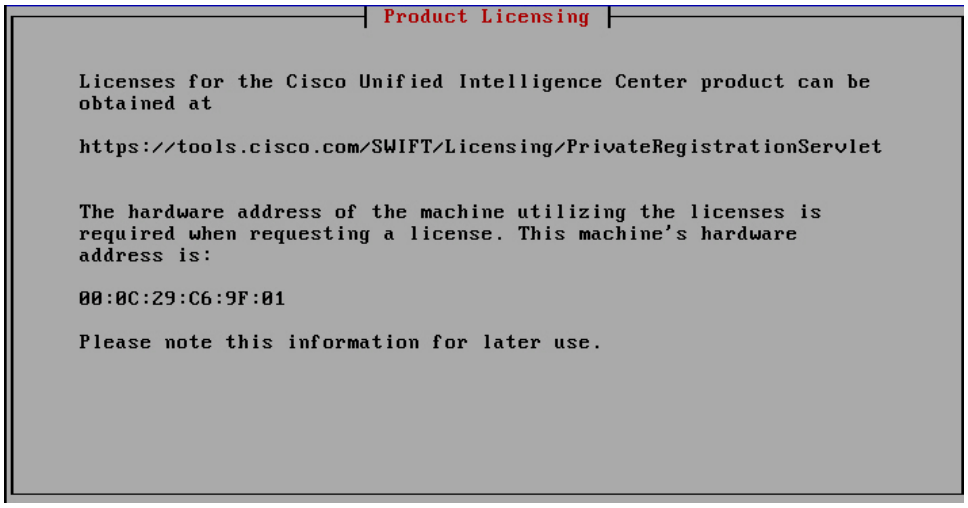
  Messages appear during the reboot, some of which prompt you to press a key. Do not respond to these prompts to press a key.

- Application Pre Install Progress Bars
- Configure and Setup Network Progress Bars

  Note: If a Network Connectivity Failure screen opens during the Configure and Setup Network process, click **Review**. Then click **OK** at the Errors screen. Follow the prompts to reenter your hostname, IP Address, and so forth. The installation will continue when the connection information is complete.

- Member Nodes only - Connection Validation message.
- Security Configuration
- Member Nodes only - A screen stating that there is a successful connection to the first node (select **Continue**).
- Member Nodes only - The SMTP Host Configuration screen(s). Select **Yes** or **No**, according to your preference.
- Member Nodes only - Platform Configuration Complete screen. Select **OK.**
- Member Nodes only - Node Type Selection screen. Select **OK**.
- Display of the Product Licensing screen.

Figure 2: License Screen



This screen shows the URL for obtaining the license (**https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet** and the Media Access Control (MAC) address. Write down this address; you will need it for the license application.

Note: The screen appears very briefly. If you do not have time to write down the MAC address before the screen close, see How Do I Find the Server MAC Address? (page 47)

- Display of Cryptographic Information screen.

Figure 3: Cryptographic Screen

- Application Post-Install Progress Bars

The installation ends at a login prompt, at which you can enter CLI commands.

To access the web interface, you need to open a browser and enter the URL *http://Controller hostname or IP/oamp* and User ID/Password of the System Application (page 54) user.

Installation Failure

Insert the DVD into the tray and perform all steps in Chapter 2 (page 11), starting with the Media and Hardware Check (page 15) and proceeding through to the First Node Configuration screen (page 18).

If a critical error occurs during installation, you are prompted to collect log files. To do this, insert a USB memory key in any available USB port and follow the instructions on the screen. See What Do I Do if the Installation Fails? (page 55).

If the installation fails over a Virtual Machine, see What Do I Do if the Installation Fails? (page 55).

After the Installation

The action to take when the installation completes depends on the type of node you installed.

Note: After installing the CUIC, depending on the version (either 7.5 or 8.x) the user should import the UCCE templates from the cisco website **cisco website** (http://www.cisco.com/cisco/software/
release.html?mdfid=282163829&flowid=5228&softwareid=282377062&release=8.5.3&relifecycle=&reltind=AVAILABLE&reltype=latest).

If	Then
If you have installed a Controller, and your cluster consists of a Controller node only	The installation is complete. 1. Open a browser and enter the URL for your Controller (*http://Controller hostname or IP/oamp*). This opens the Administration Console. Sign in using the System Application (page 54) credentials. 2. Upload the license. (page 29)
If you have installed a Controller, and you intend to install a Member	1. Open a browser and enter the URL for your Controller (*http://Controller hostname or IP/oamp*). This opens the Administration Console. 2. Sign in using the System Application (page 54) credentials. 3. Upload the license. (page 29). 4. Define the Member node (page 30) in the Administration console.
If you have installed a Member node	Open a browser and enter the URL for your Member *http://Member hostname or IP/cuic*. This opens the Unified IC Reporting web page. Sign in using the System Application (page 54) credentials. Until other users are added or integrated, the System Application user has full access to the Unified IC Member nodes.

Chapter 6

Sign in to the Administration Console

After you install the Controller, you must sign in to the Administration Console to perform tasks as explained in this chapter.

To sign in, open a browser and enter the URL for your Controller (*http://<HostAddress>/oamp*), where HostAddress is the host name or IP Address of the *Controller*. This opens the Administration Console.

Sign in using the System Application (page 54) credentials.

This chapter contains the following topics:

- Upload the License, page 29
- Define the Member Node in the Administration Console, page 30
- Verify the Controller is Synchronized with the NTP Server, page 31

Upload the License

You have limited functionality on the Administration Console and no access to the Unified IC Reporting interface until you upload the license file.

To upload the license:

1. Sign in to the Administration Console and select **Cluster Configuration > License Management**.

2. Select **Upload license file (Browse)** and navigate to the local directory where your license is stored.

   Then click **Apply License** to load the license.

See also Licenses (page 50).

Define the Member Node in the Administration Console

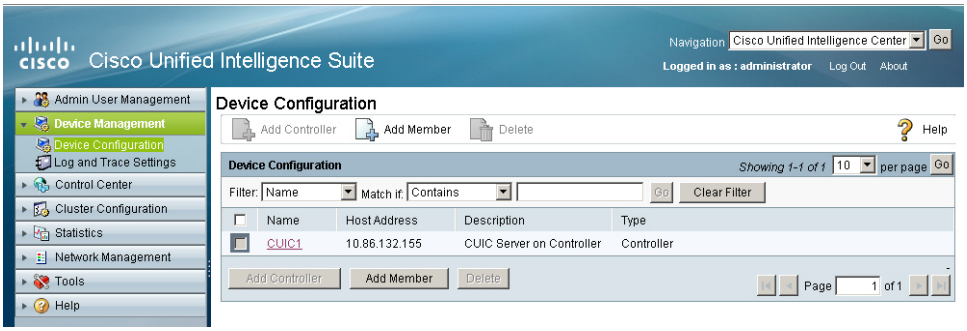
If you intend to add a Member node, you must define the Member in the Administration console before you run the installation for the Member.

Step 1 To access the Administration console, direct a browser to the URL **`http://<HOST ADDRESS>/oamp`** where HOST ADDRESS is the IP Address or Hostname of your server.

Step 2 Sign in using the system application user ID and password that you defined during installation. Refer to your Configuration Worksheet (page 7).

Step 3 From the panel in the left, select the **Device Management** drawer. Then select **Device Configuration**.

Figure 4: Device Configuration



The Device Configuration page shows the Controller that you have installed. Note that the hostname defaults to the alias CUIC1. (You can change it.)

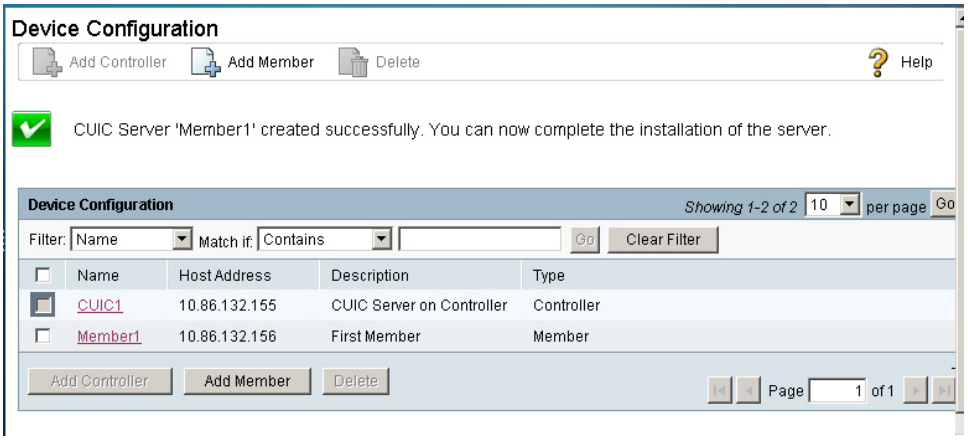
Step 4 On the Device Configuration page, click **Add Member**.

Step 5 On the Device Configuration fields for the new Member, enter a name by which you can identify the Member, the hostname or IP address, and a description for the device.

Step 6 Click **Save**.

The Member appears on the Device Configuration list.

Figure 5: Member Configured



Verify the Controller is Synchronized with the NTP Server

Make sure that the Network Time Protocol (NTP) on the Controller node is synchronized with the NTP server before you install the Member node.

To do this:

1. Access the Command Line Interface on the Controller node directly, by using the monitor and keyboard at the server console.

   At the login prompt:

   – Enter the ID for the System Administrator (page 53) user (created during Basic Install configuration).

   – When prompted, enter the password for the System Administration user.

2. Enter this command: *utils ntp status*.

   The output must indicate that the node is synchronized with an NTP server. If the Controller node is not synchronized with an NTP server, the installation of the Member node will fail.

Now that the Member is defined in Device Configuration and the NTP synchronization is verified, you can begin to configure and install (page 33) that member.

Verify the Controller is Synchronized with the NTP Server

Chapter 7

Configuring the Member

Begin the Installation and Configuration for the Member Node

Note: All configured nodes in a cluster must be up and running before you install a new Member node.

Completing the Configuration for the Member Node

Step 1 To install the member node over MCS Server, insert the DVD into the tray and perform all steps in Chapter 2 (page 11), starting with the Media and Hardware Check (page 15) and proceeding through to the First Node Configuration screen (page 18)

To install the member node over UCS Server, perform the steps in Chapter 2 (page 11), under the following sections:

- Deploy the Unified IC Open Virtualization Format/Open Virtual Appliance (OVF/OVA) Template on the Virtual Machine (page 12)
- Specify the Location of the Unified IC Installable (page 13)
- Install Unified IC on the Virtual Machine (page 14)

Step 2 At the **First Node Configuration Screen**, select **No.**

The First Node Configuration Warning screen opens.

This screen advises you that you must configure the server on the first node before you can proceed. You did this in Chapter 4 (page 30).

Step 3 Select **OK** at the screen.

Step 4 In the **Network Connectivity Test Configuration** screen, you have the option to verify the connection of this node to the first node (the Controller).

Note: This screen refers to the first node as the "publisher," in reference to its role in database replication. The first node *publishes* or replicates, the databases to the Member nodes, which are referred to as *subscribers* of the database replication.

Select **No** to open the First Node Access Configuration screen.

Step 5 In the **First Node Access Configuration** screen, enter connection values *for the first node (the Controller)*:

a. Host Name *of the Controller*

b. IP Address *of the Controller*

c. Security Password (enter and confirm)

d. Select **OK** to open the SMTP Host Configuration screen.

Step 6 In the **SMTP Host Configuration** screen, select whether you want to configure an SMTP host to receive platform-level emails; for example, emails about certificate expiration. This field is optional. You will configure email for report scheduling in the Administration console.

If	Then
You want to configure an SMTP Host.	Select **Yes** to open the second SMTP screen. Proceed to Step 7.
You do not want to configure an SMTP Host.	Select **No** to open the Platform Configuration Confirmation screen. Proceed to Step 8.

Step 7 In the second **SMTP Host Configuration** screen:

a. Enter the hostname or IP address for the SMTP server.

b. Select **OK** to open the Platform Configuration Confirmation screen.

Step 8 In the **Platform Configuration Confirmation** screen:

If	Then
You want to proceed.	Select **OK**. The installation begins. See Chapter 4 (page 25).
You want to revisit screens to modify the configuration.	Select **Back**

Chapter 8

Upgrades and Migrations

This section explains how to *upgrade* Unified IC software with engineering specials, minor releases, and maintenance releases as they become available and to *migrate* an older version of Unified IC Release 8.0(x) to Unified IC Release 8.5(x) running on a Virtual Machine.

An upgrade typically happens inplace and requires no hardware change whereas a migration involves change in hardware. To continue with Upgrade, see About Upgrades (page 35). To continue with migration, skip the initial tasks in this section and start with About Migrations (page 41).

To upgrade, you must obtain the upgrade executuable file (page 36) and then apply it using the Cisco Unified OS Administration application (page 37).

This chapter contains the following topics:

- About Upgrades, page 35
- Obtaining the Upgrade File, page 36
- Accessing Cisco Unified OS Administration, page 37
- Upgrading from DVD/CD , page 38
- Upgrading from Remote Filesystem, page 39
- Reverting to a Previous Version, page 40
- About Migrations, page 41
- Backing up data from the Cisco Unified IC Release 8.0(3), page 41
- Installing Cisco Unified IC Release 8.0(3) over a Virtual Machine, page 42
- Restoring the backed up data on the Cisco Unified IC Virtual Machine, page 42

About Upgrades

The upgrade takes less than one hour, and you can install upgrade software on your server while the system continues to operate.

Before starting the software upgrade, back up your system data using the Disaster Recovery System application. For more information on backup, see the **Administration Console User Guide for Cisco Unified Intelligence Center** (http://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html).

Upgrade and restart the controller node first. Then upgrade and restart the member(s). All nodes must be on the same version of Unified IC.

Two bootable partitions exist on your system: an active, bootable partition and an inactive, bootable partition. The system boots up and operates entirely on the partition that is marked as the active partition. Upgrade software installs on the inactive partition. The system continues to function normally on the active partition during the upgrade installation on the inactive partition.

When you are ready, you initiate a Switch Version action. You can do this using a CLI command **`utils system switch-version`**. You can also do it in the Cisco Unified OS Administration interface. The switch version action activates the inactive partition. The system reboots to the newly active (formerly inactive) partition that is running the new upgrade software. The pre-upgrade version of the software is in the inactive partition and remains there until the next upgrade.

Your configuration information migrates automatically to the upgraded version in the active partition.

Note: Database changes are stored on the database in the active partition. The database on the inactive partition does not get updated. If you make changes to the database after an upgrade and then decide to revert to the pre-upgrade software on the inactive partition, you must repeat those changes after switching the partition. See also How is Data Handled During an Upgrade? (page 50)

Obtaining the Upgrade File

You might receive an upgrade file directly from Cisco Systems, but in most case, you need to download the file from the Cisco Systems web page.

Note: The download process on Cisco.com changes periodically. The process descibed below was in place at the time this Installation Guide was prepared.

To download from the Cisco Systems website:

1. Point your browser to **http://www.cisco.com**
2. Select **Support > Download Software**.
3. Select Voice and Unified Communications.
4. Click the Customer Contact folder to expand it.
5. Click the Cisco Unified Contact Center Products folder to expand it.
6. Expand Cisco Unified Contact Center Products.

7. Click Cisco Unified Intelligence Suite and Intelligence Center Software. This opens a tree of all releases.
8. Navigate to the folder and subfolder for the release you want.
9. Select the .exe file and click **Download Now**.
10. Log in.
11. Review the download cart, select the Release Note document
12. Scroll down to select **Proceed with Download**.
13. Click **Agree** at the Download Rules page.
14. Select the download option and download /save the file to the location where you want to save it.

    Note:

    - Do not rename the patch file before you install it because the system will not recognize it as a valid file
    - Do not unzip or untar the file. If you do, the system may not be able to read the upgrade files.

15. Make this file available on all nodes.

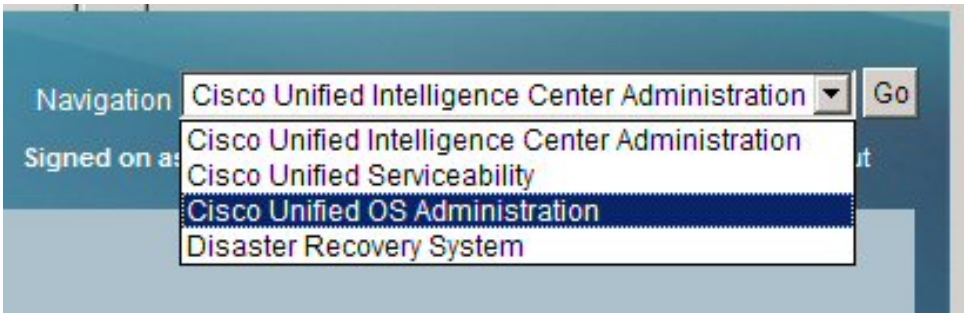
Accessing Cisco Unified OS Administration

You perform the upgrade from Cisco Unified OS Administration.

1. You can access the Cisco Unified OS Administration application:

   – From the controller node, select OS Administration from the Navigation dropdown menu and click **Go.**

Figure 6: Unified OS Administration

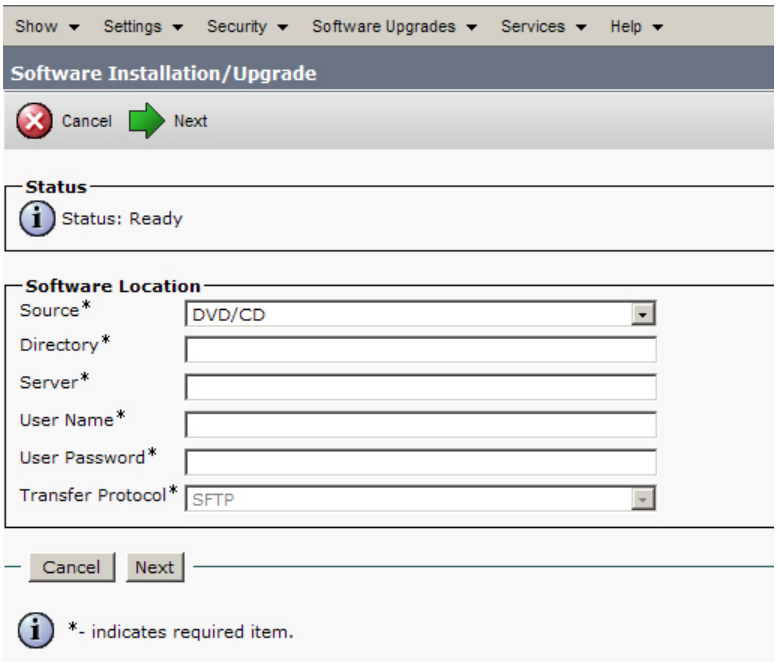


   – From a member node, enter http://x.x.x.x/cmplatform where x.x.x.x is the IP address of the member.

2. Sign in using the User Name and Password of the System Administrator account (page 53).

3. Select **Software Upgrades** > **Install/Upgrade** to display the Software Installation/Upgrade page.

Figure 7: Software Upgrade page



4. Select source: DVD/CD (page 38) or Remote Filesystem (page 39).

Upgrading from DVD/CD

Follow these steps if DVD/CD is the source for your Install/Upgrade.

Step 1 Prepare a writeable DVD and insert it into the disc drive on the server that is to be upgraded.

Step 2 Select DVD/CD from the Source list on the **Software Upgrades** > **Install/Upgrade** page.

Step 3 In the Directory field, enter the path to the upgrade file.

If the file is in the root directory, enter a slash (/) in the Directory field.

Step 4 To continue the upgrade process, click **Next.**

Step 5 Choose the upgrade version that you want to install and click **Next.**

Step 6 In the next window, monitor the progress of the download. If you encounter difficulties, refer to What To Do if the Upgrade Stalls (page 56).

Step 7 When the download completes, Click **Next.**

Step 8 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.

Step 9 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following:

a. Choose **Do not reboot after upgrade.**

b. Click **Next.**The Upgrade Status window displays the Upgrade log.

c. When the installation completes, click **Finish.**

d. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software.

Note: It takes about a half-hour to complete the Switch Version and the restart.

Step 10 Clear the browser cache before you start working on the new version of CUIC. Refer to your browser specific documentation to know more about clearing the cache.

Upgrading from Remote Filesystem

Follow these steps if Remote Filesystem is the source for your Install/Upgrade.

Step 1 Choose **Remote Filesystem** from the Source list on the **Software Upgrades > Install/Upgrade** page.

Step 2 Enter the path to the directory that contains the patch file on the remote system in the Directory field.

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, enter **/patches**. If the upgrade file is located on a Windows server, check with your system administrator for the correct directory path.

Step 3 In the **Server** field, enter the server name or IP address.

Step 4 In the **User Name** field, enter your user name on the remote server.

Step 5 In the **User Password** field, enter your password on the remote server.

Step 6 Select the transfer protocol from the **Transfer Protocol** field.

Step 7 To continue the upgrade process, click **Next.**

Step 8 In the next window, monitor the progress of the download. If you encounter difficulties, refer to What To Do if the Upgrade Stalls (page 56).

Step 9 When the download completes, click **Next.**

Step 10 If you want to install the upgrade and automatically reboot to the upgraded partition, choose **Reboot to upgraded partition**. The system restarts running the upgraded software.

Step 11 If you want to install the upgrade and then manually reboot to the upgraded partition at a later time, do the following:

a. Choose **Do not reboot after upgrade.**

b. Click **Next.** The Upgrade Status window displays the Upgrade log.

c. When the installation completes, click **Finish.**

d. To restart the system and activate the upgrade, choose **Settings > Version**; then, click **Switch Version**.

The system restarts running the upgraded software.

Note: It takes about a half-hour to complete the Switch Version and the restart.

Step 12 Clear the browser cache before you start working on the new version of CUIC. Refer to your browser specific documentation to know more about clearing the cache.

Reverting to a Previous Version

After upgrading, you can revert to the software version that was running before the upgrade, by restarting your system and switching to the software version on the inactive partition.

There are two ways to do this. You can use the CLI command **`utils system switch-version`** on each node. You can also use the user interface in the Unified Operating System Administration.

Follow these steps to revert using Unified OS Administration.

Note: All nodes must be running the same version of Unified IC. Reverting is an all-or-none operation when you operate a cluster of Unified IC nodes.

Step 1 Open the Cisco Unified Operating System Administration console directly from the controller by entering the following URL from the member: Open Cisco Unified Operating System administration console directly by entering the following URL: https://server-name/cmplatform, where server-name is the hostname or IP address of the member node.

Step 2 Sign in using System Administrator account (page 53) credentials.

Step 3 Choose **Settings > Version.**

This opens the Version Settings screen, which shows the software version on both the active and inactive partitions. To switch versions and restart, click **Switch Versions**. When the system restarts, it boots to the now-active (formerly inactive) partition with your migrated data in place.

Note: It takes about a half-hour to complete the Switch Version and the restart.

About Migrations

As part of the migration, you must first upgrade your old Unified IC Release 8.0(1) or 8.0(2) to Unified IC Release 8.0(3) by following the steps in About Upgrades (page 35) .

Once your Unified IC system is successfully upgraded to Unified IC Release 8.0(3), you must back up your Unified IC system data using the Disaster Recovery System application. For more information on backup, see the **Administration Console User Guide for Cisco Unified Intelligence Center** (http://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html).

This backed up data is then restored on the Virual Machine that has the latest version of Unified IC installed.

Backing up data from the Cisco Unified IC Release 8.0(3)

Perform the following tasks on the *Unified IC release 8.0(3)* running on a MCS server that you want to *migrate*, to Unified IC Release 8.0(3) running on a Virtual Machine.

Note: If you want to *upgrade* your previous release of Unified IC to Release 8.0(3) on the same hardware, you can do so by following the instructions in the About Upgrades (page 35) section.

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

Step 2 Log in to the **Disaster Recovery System** by using the same Administrator username and password that you use for Cisco Unified Communications Operating System Administration.

Step 3 Use the **Backup** menu options to set up backup devices to take back up of your data

Step 4 Run a manual backup. You can select the features to back up in the **Select Features** section. For more information, see the online help for the **Manual Backup** window.

Step 5 Note the **host name** and **IP address** of the system that you just backed up. You will use the same host name and IP address when you create a Virtual Machine instance.

Note: Be aware that your backup `.tar` files are encrypted by a randomly generated password. This password is then encrypted by using the cluster security password and gets saved along

with the backup `.tar` files. You must remember this security password or take a backup immediately after the security password change/reset.

Step 6 Use the **Backup History** to confirm that the backup was copleted without any errors. The Backup History window displays only the last 20 backup jobs.

Caution: Be aware that if the backup to the remote server is not completed within 20 hours, the backup session will time out. You will then need to begin a fresh backup.

Installing Cisco Unified IC Release 8.0(3) over a Virtual Machine

Note:

- After a successful backup is taken, shut down all of the Cisco Unified Intelligence Center nodes that need to be migrated from physical hardware to a Virtual Machine.
- The new Virtual Machine instance should have the same hostname and IP address as that of the machine from which you are migrating or else the DRF data restore will not be successful.

Refer to Chapter 2 - Preparing to Install Unified IC on a Virtual Machine (page 11) to install Cisco Unified Intelligence Center over a Virtual Machine.

Restoring the backed up data on the Cisco Unified IC Virtual Machine

After you have taken the back up of your data and configuration from the Unified IC Release 8.0(3) running over physical hardware, you need to restore this on to the Virtual Machine running Unified IC Release 8.0(3).

In case of a multi-node cluster deployment, before you restore a cluster, make sure that all nodes in the cluster are up and communicating with the first node. You must perform a fresh install for the nodes that are down or not communicating with first node at the time of the restore.

Note: The new Virtual Machine instance should have the same hostname and IP address as that of the machine from which you are migrating.

Ensure that the Virtual Machine is up and running the latest version of Unified IC by following the tasks mentioned in Preparing to Install Unified IC on a Virtual Machine (page 15) and Beginning the Installation - All Nodes (page 11).

Step 1 Navigate to the **Disaster Recovery System**. Log in to **Cisco Unified Communications Manager Administration**, choose **Disaster Recovery System** from the **Navigation** drop-down list box in the upper, right corner of the **Cisco Unified Communications Manager Administration** window, and click **Go**.

The **Disaster Recovery System Logon** window displays.

Step 2 Log in to the **Disaster Recovery System** by using the same Administrator username and password that you use for **Cisco Unified Communications Operating System Administration**.

Step 3 Navigate to the **Backup** > **Backup Device**.

The **Backup Device List** window displays.

Step 4 To configure a new backup device, click **Add New**.

The **Backup Device** window displays.

Step 5 Enter the backup device name in the **Backup device name** field.

Step 6 Choose **Network Directory** as the backup device and provide the details of the network shared location where the previously taken Unified IC release 8.0(3) data backup is located. For details on how to take a data backup using DRF, refer to Backing up data from the Cisco Unified IC Release 8.0(3) (page 41) .

Step 7 To update these settings, click **Save**.

Step 8 Navigate to **Restore** > **Restore Wizard**. The **Restore Wizard Step 1** window displays.

Step 9 In the **Select Backup Device** area, choose the backup device from which to restore the data.

Step 10 Click **Next**. The **Restore Wizard Step 2** window displays.

Step 11 Choose the backup file that you want to restore.

Note: The backup filename indicates the date and time that the system created the backup file.

Step 12 Click **Next**. The **Restore Wizard Step 3** window displays.

Step 13 Choose the features that you want to restore.

Note: Only the features that backed up to the file you chose appear. The existing license will not work on a Virtual Machine. You need to get a different license for the Virtual Machine, based on the licensing MAC. See How to Obtain Your License (page 51) for detailed steps on obtaining licenses.

Step 14 Click **Next**. The **Restore Wizard Step 4** window displays.

Step 15 When you get prompted to choose the nodes to restore, choose all the nodes in the cluster.

Note: To know more about viewing the status of the restore, see the **Viewing the Restore Status** topic in the Online Help. Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 16 Restart the Unified IC virtual machine.

Note: Depending on the size of your database and the components that you choose to restore, the system can require a few hours to restore.

Step 17 When the restoration completes and the **Percentage Complete** field on the **Restore Status** window in the **Disaster Recovery System** shows 100 percent, begin rebooting the subsequent nodes in the cluster.

Step 18 When all the subsequent nodes have rebooted and are running the restored version of Cisco Unified Intelligence Center, reboot the first node.

Note: Database replication on the subsequent nodes may take an hour or more to complete after the publisher reboots, depending on the size of the cluster.

Step 19 Check the Replication Status value on all nodes by using the **`utils dbreplication status`** CLI command as described in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*. The value on each node should be equal to 2.

Note: If replication does not set up properly, use the **`utils dbreplication reset`** CLI command as described in the *Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*.

Step 20 Log in to the **Disaster Recovery System** by using the same Administrator username and password that you use for **Cisco Unified Communications Operating System Administration**.

Step 21 Navigate to **Restore** >**Status**. The **Restore Status** window displays. The **Status** column in the **Restore Status** window shows the status of the restoration in progress, including the percentage of completion of the restore procedure.

Step 22 To view the restore log file, click the log filename link.

Chapter 9

Frequently Asked Questions about the Installation

This chapter contains the following topics:

- Can I Install on a Virtual Machine?, page 45
- Can My Cisco Support Provider Log In to Assist Me?, page 46
- Error Message about "No Such File or Directory", page 46
- How Do I Access Log Files?, page 46
- How Do I Add or Replace a Device in the Cluster?, page 47
- How Do I Find the Server MAC Address?, page 47
- How Do I Sign In to the Administration Console?, page 47
- How Do I Sign In to Unified IC Reporting?, page 48
- How Do I Switch Between the Administration Console and Unified IC Reporting?, page 48
- How Do I Access the Command Line Interface?, page 48
- How Do I Test Server Connectivity? , page 49
- How Do I Use the Recovery Disk?, page 49
- How Do I Uninstall?, page 49
- How is Data Handled During an Upgrade? , page 50
- Is Unified IC Supported in a Hosted Deployment?, page 50
- Unified IC Licenses, page 50
- What Accounts and Passwords are Defined During the Installation?, page 53
- What if the Installation Fails?, page 55
- What To Do if the Upgrade Stalls, page 56
- Where is a Fresh Installation Installed?, page 56
- Where is an Upgrade Installation Installed?, page 56

Can I Install on a Virtual Machine?

Starting with Release 8.0(3), you can install Unified IC on a virtual machine. You can also migrate from the previous releases of Unified IC Release 8.0(1) or 8.0(2) to a virtual machine running Unified IC Release 8.0(3).

Can My Cisco Support Provider Log In to Assist Me?

Yes. There is a utility that allows Cisco technicians to troubleshoot your system, its configurations, and databases.

You can set up and enable a time-limited access account to your system using the CLI commands under the **`utils remote_account`** command.

You can also implement this utility from the Cisco Unified Operating System Administration Console (select **Services > Remote Support**).

The procedure to do this is documented in the online help for the Cisco Unified Operating System Administration Console.

Error Message about "No Such File or Directory"

During installation on some servers, you might see an error similar to this:

```
rmmod: ohci_hcd: no such file or directory
```

This is a benign message related to USB driver modules and can be safely ignored.

The installation attempts to delete all modules on the server before loading new ones. If a module does not exist on the server where the installation is running, a message indicates that there is no such file to be deleted. Messages differ slightly for different driver names.

How Do I Access Log Files?

If you encounter problems with the installation, you can obtain and examine the install log files by entering the following commands in Command Line Interface.

- To obtain a list of all install log files from the command line, enter the CLI command **`file list install *`**.
- To view the log file from the command line, enter the CLI command **`file view install <log_file>`** where **`log_file`** is the log file name.

Other ways to access log files are as follows:

- Using the CLI **`file dump`** commands.
- Using the Syslog Viewer in the Real-Time Monitoring Tool (RTMT). You can download RTMT from the Administration console. (**Tools > RTMT Plugin Download**)

How Do I Add or Replace a Device in the Cluster?

To add a device (for example, to add an additional Member to the cluster):

1. Verify that the new or replacement device meets the hardware requirements outlined in the Hardware and System Software Specification (Bill of Materials).
2. Make sure that the other devices in the cluster are up and running.
3. Run a fresh (DVD) installation on the new or replacement device. It must be the same version of Unified IC that is currently installed on all other nodes.
4. Apply any upgrades and updates to the device so that it is running the same software as the other devices in the cluster.
5. Test that the new device can connect to the other devices in the cluster. See the FAQ on testing connectivity (page 49).

How Do I Find the Server MAC Address?

You must supply the MAC address of the Controller node when you apply for a license to operate Unified IC.

The MAC Address appears online at the end of the installation. If you do not have time to write it down, you can find it through the Command Line Interface, once the install is complete, as follows:

1. Sign in, using the credentials of the Controller System Administration user (page 53).
2. Enter this CLI Command: *show status*.

How Do I Sign In to the Administration Console?

Direct a browser to the URL for the Administration console. The URL is *http://<HOST ADDRESS>/oamp* where HOST ADDRESS is the IP Address or Hostname of your Controller node.

Enter the System Application user ID and password that you defined during installation. This person is the initial, default Super User.

Any Super Users who were added after the installation can also log in.

How Do I Sign In to Unified IC Reporting?

There are two ways to do this:

1. From the browser:
   - Direct a browser to the URL for the Reporting application. The URL is *http://<HOST ADDRESS*where HOST ADDRESS is the IP Address or Hostname of your Member node.
   - Enter your login credentials.
2. From the Administration Console:
   - Open the Control Center page.
   - Locate the Member you want to access.
   - Click the Member name to open the sign in page for that Member.
   - Enter your login credentials.

The System Application user ID and password defined during installation can log in to the Reporting application. Any additional Login Users who have been created and authenticated can also log in.

How Do I Switch Between the Administration Console and Unified IC Reporting?

If you are signed in to the Administration Console and wish to redirect your browser to the Unified IC Reporting web page:

1. Open **Control Center** > **Device Control**.
2. Locate the Member node you want to access.
3. Click the name for that Member node. The name is a link that opens the sign in page for the node.
4. Enter your login credentials.

How Do I Access the Command Line Interface?

You can access the CLI directly from any node, using the monitor and keyboard at the server console.

1. Enter the ID for the System Administrator account created during install. See What Accounts and Passwords are Defined During the Installation? (page 53)
2. When prompted, enter the password for the System Administrator account.

The CLI is documented in the **Administration Console User Guide for Cisco Unified Intelligence Center** (http://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html).

How Do I Test Server Connectivity?

There is a step to test network connectivity (page 34) during the installation of the Controller and Member servers. You can also run a basic check that one server can connect to another using this CLI command: *utils network ping*.

How Do I Use the Recovery Disk?

The installation package includes a Recovery Disk on CD media.

The purpose of this disk is to help you to recover from a catastrophic failure, such as an unbootable system.

To use the Recovery Disk, insert it into the tray and boot up into it.

The Recovery Disk has the following options:

- [S] /[s]: Swaps the active and inactive partitions (that is, boots the system with the earlier active version, which is currently inactive). This option is displayed only if there is a valid inactive partition in the system.
- [W]/[w]: Windows Pre-Installation Set-up. Reimages the system and prepares it for a Windows installation.
- [F]/[f]: Checks the file system and automatically corrects it.
- [M]/[m]: Checks the file system and manually corrects it.
- [V]/[v]: Verifies the disk partitioning layout and displays the disk partitions on the screen.
- [Q]/[q]: Quits the recovery disk program and asks you to reboot the system.

How Do I Uninstall?

There is no way to uninstall other than reinserting the installation DVD, which will reformat the hard disk.

How is Data Handled During an Upgrade?

Data migration occurs during an upgrade installation (page 56). This includes the database, configuration properies, and licensing files.

Warning: Do not make configuration changes from the start of the upgrade process until you have activated the inactive partition and rebooted the system.

If you decide to downgrade and switch/restart the system to the *inactive* partition that contains the *older version* of the software, any configuration changes that you made since upgrading will be lost.

Is Unified IC Supported in a Hosted Deployment?

Deployment in a hosted environement was not qualified and tested in this release. For testing, each Unified IC instance was dedicated to a single customer.

Qualification for a hosted contact center is planned for a future release.

Unified IC Licenses

Unified IC licenses are "node-locked." This means a license is "locked to" the MAC address of the Controller node. A MAC address change will require a new license.

For Unified IC installations on Virtual Machines, the license is locked to the licensing MAC of the Virtual Machine. The licensing MAC is different from the physical MAC address of the system. The licensing MAC string is generated during installation and is based on various input fields, such as the hostname, IP address, and so forth.

A licensing MAC address change will require a new license. The license file is physically located on the Controller node and is distributed to all members nodes in the cluster through database replication.

There can be only one license installed on a system at any point in time.

Uploading the license file is the first action the System Application User must take after installing the Controller node.

After installation, and until the System Application User obtains and uploads a Standard or Premium license, he or she:

- Can sign in to the Administration Console to view the Controller and to add the alias name.
- Cannot perform other Administration Console functions.
- Cannot sign in to the Unified IC Reporting application.

- Cannot install member nodes.

How To Obtain Your License

To acquire a license:

1. Go to the Cisco Product License Registration website at this URL: **https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet**
2. If you do not have a PAK, click the **available licenses link** (https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?DemoKeys=Y).
3. Scroll to Voice Products and click **Cisco Unified Intelligence Center - v8.0**.
4. Enter your MACAddress as a single string (with no spaces between the characters), accept the agreement, and enter your Registrant Information.

   In the case of Cisco Unified IC installation over Virtual Machine, you need to provide the licensing MAC. See Locating the MAC Address (page 51).
5. Follow prompts to complete the registration pages.

You will receive the license file in an email from Cisco Systems. When you receive it, save it locally in a location where it cannot be deleted by mistake or opened by an unauthorized person. In the event that your system becomes corrupted, you can browse to this location to upload the license file again.

The same license file will be valid if you need to reapply it - unless you apply it to a new server with a new MAC address.

Caution: License files are human-readable and can be opened. However, changing any text in the license file invalidates the license.

Locating the MAC Address

You must supply the MAC address of the Controller node when you apply for a license to operate Unified IC.

The MAC Address appears online at the end of the installation. If you do not have time to write it down, you can find it through the Command Line Interface, once the install is complete, as follows:

1. Sign in, using the credentials of the System Administration user.
2. Enter this CLI Command: *show status*.

How to Upload the License

Upload the license in the Unified IC Administration interface.

To do this, select **Cluster Configuration** > **License Management** . Refer to the online help for instructions.

License Types

Unified Intelligence Center has four license types: Demo, Lab/Trial, Standard, and Premium.

TYPE	EXPIRATION	NODES	USERS	FEATURES
DEMO/LAB	Valid for 90 days. Can be extended for one additional 90-day session with a reinstallation of Unified IC.	Controller and all Member nodes (a maximum of 8 nodes).	No limit	Premium feature set
TRIAL	Valid for 90 days.	Controller node only	No limit	Premium feature set
STANDARD	Has no expiration/timeout.	Controller and all Member nodes (a maximum of 8 nodes).	Unlimited but requires system sizing for optimum performance. See the Sizing Tool for guidelines.	Standard feature set
PREMIUM	Has no expiration/timeout.	Controller and all Member nodes (a maximum of 8 nodes).	Unlimited but requires system sizing for optimum performance. See the Sizing Tool for guidelines.	Premium feature set

See Standard and Premium feature set. (page 52).

Feature Set for Standard and Premium Licenses

This table compares the Unified IC features that are offered with the Standard and the Premium license.

Feature	Standard	Premium
Core reporting with standard reports (print, save, clone, export to Excel, export as XML)	✓	✓
Dashboards	✓	✓
Cisco stock templates	✓	✓

Feature	Standard	Premium
Import and run reports created with Intelligence Center Premium	✓	✓
Change report filters (date, time, items in category)	✓ with Save As	✓
Rename columns	✓ with Save As	✓
Add computed fields to Report Definitions	-	✓ with Save As
Create or modify Report Definitions queries to build new reports	-	✓ with Save As
Create Drilldowns in the Report Definition	-	✓
Rename columns	✓ with Save As	✓
Reorder, hide, unhide report columns	✓ with Save As	✓
Create Thresholds	✓ with Save As	✓
Scheduled reports on dashboards	✓	✓
Add computed fields to Report Definitoins	-	✓ with Save As
Partitioning by collections	✓	✓
XSLT	-	Future Release
RSS	-	Future Release
Permalinks	✓	✓
Access to non-Cisco data sources	-	Future Release
Data Migration from Release 7.5(x)	N/A	Future Release

What Accounts and Passwords are Defined During the Installation?

During the installation, you specify three passwords: the System Administrator user, the System Application user, and the database access security password. All three must start with an alphabetic character, must be at least six characters long, and can contain alphanumeric characters, hyphens, and underscores. Only one of these (the *application user* and password) is passed to the online Administration console.

- **System Administrator account**

  The System Administrator account User ID and password are configured at installation for each node. It is a best practice to enter the same user name and password for all nodes.

The System Administrator for the *Controller* can access:

– The CLI for the Controller.

– The Cisco Systems tools on the Navigation dropdown in the Administration console: Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified OS Administration interfaces.

The System Administrator has no access to functions in the Unified IC reporting application.

Note: If you configure unique System Administrator credentials for Member nodes, you must use those credentials to access the CLI for those Member servers only.

- **System Application User account**

  The System Application account User ID and password are configured at installation for each node. It is a best practice to enter the same user name and password for all nodes.

  The System Application user name and password that are configured for the *Controller* allow an initial login to the Administration console. This user becomes that initial Super User and, once the license is applied, can log in to the Unified IC Reporting application on all Member nodes.

  As the initial Super User, the System Application User can create additional Super Users in the User Management screen or by using the CLI command **`set account`**. This user can also sign in to the Unified IC Reporting interface with full access to all functions.

  The initial Super User (the System Application user) created in the installation does not need to be set up in Active Directory.

  Any additional Super Users created through the Administration console are considered to be IMS users. They can sign into Unified IC Reporting and will be limited to the Login User role until they are given additional privileges.

  Note: If you configure unique System Application credentials for Member nodes, those users have no login rights.

- **Security Password**

  The security password defined in the installation wizard is used by the system for the database security password to authorize communications between devices. This password is identical on all servers in the cluster. The security password is also used by the Disaster Recovery System (DRS) for encryption of the backup file.

  You can change the security password using the CLI command **`set password security`**.

What if the Installation Fails?

If the installation fails, you see a screen asking if you want to copy diagnostic information to a device.

Figure 8: Installation Failed Screen

Insert a USB key.

Select **Yes.**

Select **Continue** at the next two screens.

Note: The CLI command to view the install logs is file view install. The CLI is documented in the **Administration Console User Guide for Cisco Unified Intelligence Center** (http://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html)

If the installation fails over a Virtual Machine, you see a screen asking if you want to copy diagnostic information to a device.

How to Dump Install Logs to the Serial Port of the Virtual Machine

Step 1 Configure a serial port on the Virtual Machine.

While the Virtual Machine is powered OFF, edit settings and add a serial port to the Virtual Machine. You cannot add a serial port while the Virtual Machine is running. Attach the serial port to a .tmp file, and then power on the Virtual Machine and start the install.

Step 2 When you are ready to dump the log files, attach a new, empty file to the serial port.

If the system halts due to an install failure and asks if you want to dump the logs, *before* you answer yes, you must edit settings on the Virtual Machine and attach the actual file name where you want to dump the logs. The reason for originally attaching the .tmp file to the serial port is that during the boot-up of Linux, a few garbage characters (terminal escape sequences) get

output to that port. If you dump the logs into that file, these characters will corrupt the .tar format of the file. In order to create a valid .tar file, you must connect the serial port to a new and empty file just before you dump the logs to it.

Step 3 Return to the Virtual Machine console and proceed to dump the logs to the serial port. After the file is complete, open it with 7-zip, which you can download from **http://www.7-zip.org/download.html**.

Step 4 Important: After a successful install, power off the Virtual Machine, edit settings, and remove the serial port from the Virtual Machine. Leaving the serial port (or any other virtual hardware) can negatively impact performance of the Virtual Machine. The serial port has no other use other than dumping the install logs and you will not need it again, unless you perform a fresh install.

What To Do if the Upgrade Stalls

During the installation of upgrade software, the upgrade may appear to stall. The upgrade log stops displaying new log messages. When the upgrade stalls, you must cancel the upgrade, disable I/O throttling, and restart the upgrade procedure. When you successfully complete the upgrade, you do not need to reenable I/O throttling.

To disable I/O throttling, enter the CLI command *utils iothrottle disable*.

To display the status of I/O throttling, enter the CLI command *utils iothrottle status*.

To enable I/O throttling, enter the CLI command *utils iothrottle enable*. By default, iothrottle is enabled.

If the system does not respond to the cancellation, you must reboot the server, disable I/O throttling, and restart the upgrade process procedure.

Where is a Fresh Installation Installed?

All Controller servers have an active bootable partition, an inactive bootable partition, and a common partition.

The installation creates these partitions, and a fresh (first-time) installation places the new software and operating system on the *active* partition. The system boots up and operates on the *active* partition.

Where is an Upgrade Installation Installed?

All Controller servers have an active bootable partition, an inactive bootable partition, and a common partition.

Upgrade versions are installed on the *inactive* partition.

To complete the upgrade, you switch partitions.

You do this using the CLI command **`utils system switch-version`**.

You can also do this from the Cisco Unified Communications Operating System Administration screen. Navigate to **Settings > Version**. This opens the Version Settings screen, which shows the software version on both the active and inactive partitions. To switch versions and restart, click **Switch Versions**. When the system restarts, it boots to the now-active (formerly inactive) partition with your migrated data in place.

See also: Software Upgrades (page 35)

Where is an Upgrade Installation Installed?

Index

Administration console
- adding member node....*30*
- logging in....*29*, *47*
- uploading license....*29*

auto-negotiation....*17*

basic install wizard
- auto-negotiation settings....*17*
- case sensitivity....*6*
- configuration worksheet....*7*
- DHCP setting....*18*
- DNS settings....*18*
- MTU setting....*17*
- network settings....*18*
- NIC speed and duplex settings....*17*
- NTP settings....*21*
- SMTP settings....*22*
- timezone check....*17*
- user interface....*9*

case sensitivity....*6*

certificate information....*7*, *18*

Cisco Unified Administration....*54*

Cisco Unified Intelligence Center
- in hosted deployment....*50*
- license....*6*, *29*
- operating system....*5*
- remote access for technical assistance....*46*
- uninstalling....*49*
- version....*16*

Cisco Unified OS Administration
- accessing....*37*
- and migration....*41*
- and upgrades....*35*
- switch version....*40*

Cisco Unified Serviceability....*54*

CLI
- access to....*48*, *54*
- changing configuration after installation....*17*
- documentation....*48*
- system administration user....*31*

configuration
- changing in CLI....*17*
- first node (controller)....*21*
- member nodes....*33*

controller node....*5*
- configuration....*21*
- logging in....*47*

DHCP....*18*

Disaster Recovery System....*54*

DNS servers
- configuring at installation....*18*

domain....*18*

DVD media....*15*

failure
- of hardware sanity check....*16*
- of installation....*27*, *55*
- of media check....*15*

gateway....*18*

hardware
- failure of sanity check....*16*
- MAC address....*26*
- sanity check....*16*

hosted deployment....*50*

hostname....*18*

installation
- and partitions....*56*
- DVD....*15*
- error messages....*46*

failure....*27*, *55*
length of....*8*, *25*
log files....*27*, *46*, *55*
on re-purposed server....*6*
on virtual machine....*45*
processes....*25*
Product Licensing screen....*26*
sequence....*8*
uninstall....*49*
user accounts....*53*
user interface....*9*
IP address and mask....*18*
license
best practices....*50*
feature set by license type....*52*
obtaining....*51*
Product Licensing screen....*26*
types....*52*
uploading....*29*
log files....*46*
login information
application user....*48*
system administrator user....*53*
system application user....*30*, *47*
MAC Address....*26*, *47*, *51*
media check....*15*
failure....*15*
member node
adding in Administration console....*30*
defining in operations console....*30*
installing and configuring....*33*
maximum allowed....*5*
network connectivity test....*34*
sequence of installation....*6*
migration....*35*
migrations
and backups....*41*
length of....*41*
MTU....*7*, *17*
network connectivity....*34*, *49*
network settings....*18*
Network Time Protocol (NTP)....*21*
NIC duplex setting....*17*
NIC speed....*17*
NTP server....*8*, *21*
partitions
active and inactive....*36*, *56*
passwords
configured at installation....*53*
security....*7*, *22*, *54*
system administrator user....*53*
system application user....*22*, *54*
ping....*49*
Premium license feature set....*52*
Product Licensing screen....*26*
Real-Time Monitoring Tool....*46*
recovery disk....*49*
remote access....*46*
security password....*7*, *8*, *22*, *54*
servers
adding or replacing....*47*
DNS....*18*
hostname....*18*
IP address and mask....*18*
NTP....*21*
SMTP....*22*, *34*
SMTP Host....*22*, *34*
Standard license feature set....*52*
switch version....*40*, *56*
system administrator user....*7*, *18*

and CLI access....*48*
configuring at installation....*53*
system application user....*8*, *22*, *30*, *54*
configuring at installation....*22*
password....*22*, *47*, *48*
timezone....*17*
UBS B Series/C Series
installation....*11*
Unified IC reporting interface
logging in....*48*
uninstall....*49*
upgrade files
accessing....*36*
upgrades....*16*, *35*, *50*, *56*
and backups....*35*
from DVD....*38*
from remote filesystem....*39*
length of....*35*
troubleshooting....*56*
user accounts
configured at installation....*18*, *53*
version....*16*
reverting to the prior....*40*
virtual machine
installation....*11*
virtual machines....*45*