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 UCB's 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.

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

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 this URL: http://www.cisco.com/go/trademarks. 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)

© 2003-2015 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xv

Change History xv
About This Guide xv
Audience xv
Obtaining Documentation and Submitting a Service Request xvi
Field Alerts and Field Notices xvi
Documentation Feedback xvi
Conventions xvi

CHAPTER 1 Preparation 1

Scenarios 1

Installation Scenario 1
Virtualization Installation 1

Upgrade Scenarios 1

Common Ground Upgrades 2
Technology Refresh Upgrades 2

System Requirements 3

Platform Requirements 3
Network Requirements 4
Software License Requirements 4
Virtualization Requirements 6
Compatibility Requirements 7

CHAPTER 2 Installation Overview 9

Installation Tools 9
Uninstallation 10
CHAPTER 3  

Preinstallation  11

Preinstallation Task Flow  11
Preinstallation Tasks  12
  Set up Active Directory  12
    Verify Domain Controller Health  12
      Run dcdiag.exe  12
      Run repadmin.exe  13
    Install DNS on Additional Domain Controller  14
    Configure Active Directory Sites  14
    Assign Global Catalog and Set Time Source  15
    Configure DNS Server on Forest Root Domain Controller  15

Set Up Virtual Machines  16
  Verify Datastores  16
  Download Unified CCE OVA Files  16
  Create Virtual Machines from OVA Files  17

Mount and Unmount ISO Files  18
Set Up Third-Party Software  18
  Install Microsoft Windows Server  18
  Set Windows Locale  20
  Install VMware Tools  20
  Install Microsoft SQL Server  21
    Set Users as System Administrators  24
  Install Antivirus Software  24
  Configure a Database Drive  25

CHAPTER 4  

Installation  27

Installation Task Flow  27
Installation Tasks  29
  Set Up Virtual Machines for Installation  30
    Validate Network Adapter Settings and Power On  30
    Configure Network Cards  30
    Configure Private Ethernet Card  31
    Configure Visible Ethernet Card  31
  Live Data Installation  32
Initial Configuration 69

Initial Configuration Overview 69
Initial Configuration Task Flow 69
Initial Configuration Tasks 70

Configure Cisco Unified Contact Center Enterprise 70
Access Configuration Manager tool 70
Configure Media Routing Domain 71
Configure trunk groups 71
Configure Network VRU Bank 72
Configure services 73
Configure dialed numbers 75
Configure call types 76
Configure Variables 77
Configure Expanded Call Context Variables 77
ECC Variables for Blended Collaboration or Voice MRDs with Collaboration 78
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate ECC Variable Size for CTI Server</td>
</tr>
<tr>
<td>Enable ECC Variables</td>
</tr>
<tr>
<td>Define ECC Variables</td>
</tr>
<tr>
<td>Configure User Variables</td>
</tr>
<tr>
<td>Define User Variables</td>
</tr>
<tr>
<td>Configure Users</td>
</tr>
<tr>
<td>Create Person records</td>
</tr>
<tr>
<td>Associate agents with peripherals</td>
</tr>
<tr>
<td>Assign Agent Desk Settings</td>
</tr>
<tr>
<td>Ring No Answer</td>
</tr>
<tr>
<td>Configure Agent Desk Settings</td>
</tr>
<tr>
<td>Designate agent supervisors</td>
</tr>
<tr>
<td>Create agent teams</td>
</tr>
<tr>
<td>Configure Network VRUs</td>
</tr>
<tr>
<td>Create Network VRU Target</td>
</tr>
<tr>
<td>Define Network VRU Label</td>
</tr>
<tr>
<td>Set Default Network VRU and Range of Correlation Numbers</td>
</tr>
<tr>
<td>Configure scripts</td>
</tr>
<tr>
<td>Configure Network VRU scripts</td>
</tr>
<tr>
<td>Troubleshoot Network VRU scripts</td>
</tr>
<tr>
<td>VRU error checking</td>
</tr>
<tr>
<td>Configure routing and administrative scripts</td>
</tr>
<tr>
<td>Configure Agent or Device Targets</td>
</tr>
<tr>
<td>Configure Agent Targeting Rules</td>
</tr>
<tr>
<td>Configure device targets and labels</td>
</tr>
<tr>
<td>Configure device targets</td>
</tr>
<tr>
<td>Configure labels</td>
</tr>
<tr>
<td>Configure translation routes</td>
</tr>
<tr>
<td>Configure Skill Groups or Precision Routing</td>
</tr>
<tr>
<td>Configure Skill Groups</td>
</tr>
<tr>
<td>Add skill groups</td>
</tr>
<tr>
<td>Assign skill groups as service members</td>
</tr>
<tr>
<td>Assign agents to skill groups</td>
</tr>
<tr>
<td>Configure Precision Routing</td>
</tr>
<tr>
<td>Add Attributes</td>
</tr>
</tbody>
</table>
Search for Agents 100
Assign Attributes to Agents 100
Add Precision Queue 100
Consider If Formula for Precision Queue 103
Build Precision Queue Steps 104
Configure routes 106
Perform Bulk Configuration 106
Access Bulk Configuration Tools 106
Add New Records 107
Insert New Records 107
Import Data 107
Data File Format 108
Select Data 109
Select Records 109
Select One Field in Multiple Records 109
Edit Range of Data 110
Apply a Single Value to a Range of Edit-Control Fields 110
Apply a Single Value to a Range of Selection-Box Fields 110
Apply a Range of Values to a Range of Fields in a Column 111
Configure Cisco Unified Intelligence Center 112
Acquire License 112
Sign In to Administration Console 112
Upload License 113
Configure SQL User Account 113
Configure Data Sources 114
Configure Unified CCE Data Sources 114
Create Data Source for Cisco Unified CVP Report Data 115
Download Report Bundles 116
Import Report Bundles 117
Configure Unified Intelligence Center Administration 117
Configure Cisco Unified Customer Voice Portal 118
Configure Unified CVP Server 118
Configure Network Card for Unified CVP 118
Set up Unified CVP Media Service IIS 119
Set Up FTP Server 119
Configure Unified CVP Reporting Server

Create Reporting Users

Create Superusers

Set Up Active Directory Server for LDAP Users

Sign In to Cisco Unified Intelligence Center Reporting Interface

Create Data Source and Import Report Templates

Obtain Cisco Unified CVP Report Templates

Import Unified CVP Report Templates and Set Data Source

Configure Unified CVP Operations Console

Enable Unified CVP Operations Console

Configure Unified CVP Call Server Component

Configure Unified CVP VXML Server Component

Configure Unified CVP Media Server

Install Unified CVP licenses

Configure Gateways

Add Unified CCE Devices

Add Unified Communications Manager Devices

Add Unified Intelligence Center Devices

Transfer Scripts and Media Files

Configure SNMP

Configure SIP Server Group

Configure Dialed Number Patterns

Configure Cisco Unified Communications Manager

Set Up Device Pool

Set Up Unified Communications Manager Groups

Set Up CTI Route Point

Set Up Trunk

Set Up Application User

Set Up SIP Options

Set Up Route Pattern

Set Up Conference Bridge

Set Up Media Termination Point

Set Up Transcoder

Set Up Media Resource Group

Set Up and Associate Media Resource Group List
Set Up Enterprise Parameters 135
Configure Mobile Agent 135
Configure Local Trunk 136
   Deploy SIP Trunk 137
Configure Outbound Dialer 137
Configure A-Law Codec 138
Configure Support for Multiline Agent Control 138
Configure RSM 139
   Configure Simphone Device Dependencies 139
   Create Simphone Device 141
   Associate a Line DN to Simphone Device 142
   Use Simphone Bulk Administration Tool 142
Set Up Login Pool Simphone 143
Create RSM User Group 144
Create RSM Application User 145
Set Up Agent Phone Device 145
Configure Caller-Specific Music on Hold 146
   Upload audio file 146
   Configure audio source 146
   Configure Unified CCE routing script 147
Configure Cisco Finesse 147
   Configure Contact Center Enterprise CTI Server Settings 147
   Configure Contact Center Enterprise Administration & Data Server Settings 148
   Configure Cluster Settings 149
   Restart Cisco Finesse Tomcat 150
   Check Replication Status 150
   Ensure Agents Have Passwords 150
   Ensure Logout Non-Activity Time for Agents is Configured 151
   Ensure Agents Can Sign in to Desktop 151
   Trust Self-Signed Certificate 152
   Obtain and Upload CA Certificate 154
   Configure DNS on Clients 156
   Live Data Reports 156
      Prerequisites for Live Data 156
Add Live Data Reports to Finesse 157

Add Live Data Reports to Default Desktop Layout 157

Add Live Data Reports to Custom Desktop Layout 158

Add Live Data Reports to Team Layout 160

Modify Live Data Stock Reports for Finesse 161

Initial Configuration Troubleshooting 163

---

**CHAPTER 6**

Upgrade Overview 167

Multistage Upgrades and Maintenance Windows 167

Unified CCE Contact Center Upgrade Flowcharts 170

Data Migration Considerations 177

Silent Upgrade 178

Uninstallation 178

---

**CHAPTER 7**

Common Ground Upgrade 181

Preupgrade Overview 181

Common Ground Preupgrade Task Flow 182

Common Ground Preupgrade Tasks 183

ESX Supportability 183

Disaster Recovery Plan 184

Change the SCSI Controller Type 184

Upgrade VM Network Adapters from E1000 to VMXNet3 185

VM Hardware Version Upgrade 186

Upgrade Overview 186

Common Ground Upgrade Task Flow 189

Common Ground Upgrade Tasks 192

Upgrade to Windows Server 2012 R2 192

Remove Previous Windows Installation 194

Upgrade to SQL Server 2014 194

Migrate Unified CCE Logger Database and Upgrade Logger 195

Upgrade Unified CCE Call Router 196

Migrate HDS Database and Upgrade the Unified CCE Administration & Data Server 197

Upgrade Peripheral Gateways 198

Upgrade Outbound Option Dialer 198

Upgrade Unified CCE Administration Client 199
CHAPTER 8

Common Upgrade Tasks 201
- Upgrade Voice and Data Gateways 201
- Bring upgraded Side A into service 202
- Verify operation of upgraded Side B Call Router and Logger 203
- Upgrade Cisco JTAPI Client on the Unified Communications Manager PG 205
- Database Performance Enhancement 206
  - Performance Enhancement of Logger Database 206
  - Performance Enhancement of AW-HDS Database 207

CHAPTER 9

Technology Refresh Upgrade 209
- Preupgrade Overview 209
- Technology Refresh Preupgrade Task Flow 210
  - Disable Configuration Changes 211
  - Export the Server Registry 211
- Upgrade Overview 212
- Technology Refresh Upgrade Task Flow 214
- Technology Refresh Upgrade Tasks 217
  - Migrate the Logger Database and Upgrade the Logger 217
  - Upgrade Unified CCE Call Router 219
  - Migrate HDS Database and Upgrade Unified CCE Administration & Data Server 219
  - Upgrade Peripheral Gateways 221
  - Upgrade Outbound Option Dialer 222
  - Upgrade Unified CCE Administration Client 222

CHAPTER 10

Active Directory Upgrade 223
- Migrate Active Directory and DNS 223
  - Preparing existing forest via the adprep command 223
  - Install Active Directory on New Domain Controller 223
  - Configure Active Directory sites on new domain controller 224
  - Move Flexible Single Master Operation roles 224
  - Transfer Schema Master role 224
  - Redefine the time source 225
  - Assign Global Catalogs 225
  - Configure member servers to point to new DNS servers 226
Demote current domain controllers to member servers and uninstall DNS 226

Upgrade Active Directory and DNS 227
  Upgrade Domain Controller 227
  Assign Global Catalog 227

CHAPTER 11

Testing 229
  Testing Overview 229
  Testing Tasks 229
    Verify Upgrade to Cisco Unified Customer Voice Portal 229
    Verify IOS Gateway Upgrade 230
    Verify Upgrade to Cisco IOS-Based Transcoders and Conference Bridges 231
    Verify Upgrade to Cisco Unified CCE Router and Logger 231
    Verify Upgrade to Cisco Real Time Administration Workstation, Historical Database Server 232
    Verify Upgrade to Peripheral Gateways 233
    Verify Upgrade to CTI OS Server and Outbound Option 234
    Verify Redundancy 234
    Verify Upgrade to CTI OS and Cisco Agent Desktop Agent/Desktop Clients 235
    Verify Upgrade to Cisco Unified Communications Manager 235

APPENDIX A

Live Data CLI Commands 237
  Supported Character Set for Live Data Installation CLI Commands 237
  Live Data AW DB Access 238
    set live-data aw-access 238
    unset live-data aw-access 239
    show live-data aw-access 239
  Live Data Cluster Configuration 239
    set live-data secondary 239
    unset live-data secondary 240
    show live-data secondary 240
  Live Data Reporting Configuration 240
    set live-data reporting-interval 240
    show live-data reporting-interval 241
    unset live-data reporting-interval 241
  Live Data Services Registration 242
set live-data cuic-datasource 242
show live-data cuic-datasource 242
unset live-data cuic-datasource 243
set live-data machine-services 244
show live-data machine-services 244

APPENDIX B
Certificates for Live Data 245
Certificates and Secure Communications 245
Obtain and Upload Third-party CA Certificate 246
Export Self-Signed Live Data Certificates 246
Import Self-Signed Live Data Certificates 247
Produce Certificate Internally 248
Set up Microsoft Certificate Server for Windows Server 2012 R2 248
Download CA certificate 249
Deploy Root Certificate for Internet Explorer 249
Set Up Certificate for Internet Explorer Browser 250
Set Up Certificate for Firefox Browser 251

APPENDIX C
IPv6 Configuration 253
Configure NAT64 for IPv6-Enabled Deployments 253
Configure DNS for IPv6 254
Determine IPv6 Translation of IPv4 Address for DNS Entry 254
Set Up IPv6 for VOS-Based Contact Center Applications 255
Set Up IPv6 Using Cisco Unified Operating System Administration 255
Set Up IPv6 for VOS-Based Applications Using the CLI 256
Preface

- Change History, page xv
- About This Guide, page xv
- Audience, page xv
- Obtaining Documentation and Submitting a Service Request, page xvi
- Field Alerts and Field Notices, page xvi
- Documentation Feedback, page xvi
- Conventions, page xvi

Change History

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td></td>
</tr>
<tr>
<td>Added note to Install VMware Tools topic</td>
<td>November 19, 2015</td>
</tr>
</tbody>
</table>

About This Guide

This guide describes how to install the components and software for a new Unified CCE system, or to upgrade an existing Unified CCE system.

Audience

This guide is intended for users who install and upgrade Unified CCE contact centers. The procedures assume that the system has been thoroughly designed and staged in preparation for the installation or upgrade.
Obtaining Documentation and Submitting a Service Request


Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

Field Alerts and Field Notices

Cisco products may be modified or key processes may be determined to be important. These are announced through use of the Cisco Field Alerts and Cisco Field Notices. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest.

Log into www.cisco.com and then access the tool at http://www.cisco.com/cisco/support/notifications.html.

Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

Conventions

This document uses the following conventions:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **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.  
  - A syntax value that the user must replace. Example: IF (*condition*, *true-value*, *false-value*)  
  - A book title. Example: See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* |
## Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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>` |
| `< >` | 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. |
CHAPTER 1

Preparation

- Scenarios, page 1
- System Requirements, page 3

Scenarios

Installation Scenario

Virtualization Installation

You install Cisco Unified Contact Center Enterprise (Unified CCE) in a virtualized environment. In a virtualized environment, you can run Unified CCE on a VMware ESXi platform. Run the virtual machines (VMs) on Cisco Unified Computing System (UCS) B-series or C-series servers, or equivalent third-party servers. For more information about server specifications, see the Unified Communications Virtualization Supported Applications page at http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Supported_Applications.

Install the Cisco Unified CCE components after you configure the VMs.

Related Topics
- Preinstallation Task Flow, on page 11
- Installation Task Flow, on page 27
- Initial Configuration Task Flow, on page 69

Upgrade Scenarios

There are two methods you use to upgrade your Unified CCE system:

- The Common Ground method is an in-place upgrade using your existing hardware. If your hardware meets the requirements for this release, you can perform a Common Ground upgrade without acquiring additional hardware.
• Use the Technology Refresh upgrade method to upgrade your hardware at the same time as the Unified CCE system. When using the Technology Refresh method, you prepare a destination system on new hardware and then migrate data from your existing deployment to the new one.

Upgrade scenarios are considered at a component level; you can perform one type of upgrade on one component, and another type of upgrade on another component. However, the A and B side of any given component must be running on identical hardware.

Follow the task flow and tasks for the upgrade scenario that applies to each individual component involved in the overall upgrade.

**Common Ground Upgrades**

The Common Ground upgrade for Unified CCE 11.0(x) supports in-place upgrade of the Operating System, followed by the upgrade of Unified CCE from previous releases.


Additionally, ensure that there is sufficient hard disk space to support the new release. For more information, see [http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE](http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE).

If your existing system does not meet the system requirements for Release 11.0, upgrade the hardware, and then perform a Technology Refresh upgrade instead.

The supported paths for Common Ground upgrades are:

- Release 10.0(x) to Release 11.0(x)
- Release 10.5(x) to Release 11.0(x)

**Related Topics**

- [Common Ground Preupgrade Task Flow](#), on page 182
- [Common Ground Upgrade Task Flow](#), on page 189

**Technology Refresh Upgrades**

To perform a Technology Refresh upgrade, you first prepare the destination system using new hardware, and then migrate configuration data from your existing production system. This method reduces the maintenance window required for the upgrade process compared to a Common Ground upgrade.

The supported paths for Technology Refresh upgrades are:

- Release 10.0(x) to Release 11.0(x)
- Release 10.5(x) to Release 11.0(x)

This release supports only a virtualized environment.

Follow the documented procedures to build a parallel network using new hardware and pre-stage it with configuration data to support the existing production network. Use the Enhanced Database Migration Tool (EDMT) to transfer data and perform a schema upgrade during the upgrade process. Do not use backup and restore procedures to perform the pre-staged configuration on the parallel network.
System Requirements

Before you start installation or upgrade activities, fully plan your Unified CCE contact center installation or upgrade. Ensure that the system is ready, and meets all requirements for supported hardware and software. This section provides a summary of the requirements for Unified CCE. If you have not confirmed all the information in this section, complete the planning phase before proceeding further.

Platform Requirements

Server selection for Unified CCE in a virtualized environment involves several factors, including:

- The server and all related hardware must be supported for use in a virtualized Unified CCE system
- Minimum specifications for processing, memory, and storage
- Whether you want a packaged and tested Cisco configuration (Tested Reference Configuration or TRC) or a configuration that you base on Cisco-defined minimum requirements (Specs-based Configuration)
- Compatibility requirements for all hardware, and Cisco and third-party software including the VMware required to run and manage a virtual environment

Confirm that your hardware selection is supported for Unified CCE and meets all minimum specifications:

<table>
<thead>
<tr>
<th>Server</th>
<th>VMware required</th>
<th>For detailed requirements information, see</th>
</tr>
</thead>
</table>
| UCS B- or C-series (TRC): | • VMware vSphere ESXi  
| UCS B- or C-series (Specs-based): | • VMware vCenter  
|                          | • VMware vSphere ESXi              |                                           |
| Third-party (Specs-based): | • VMware vCenter  
|                           | • VMware vSphere ESXi              |                                           |

In addition to confirming that your servers meet minimum specifications, confirm that your server choice is compatible with all Cisco and third-party software.
Related Topics

Compatibility Requirements, on page 7

Network Requirements

Network requirements for virtualized Unified CCE systems vary widely, depending on the size and type of Unified CCE solution deployment. Confirm that you have clearly established all network requirements before you install or upgrade a Unified CCE contact center.

Related Topics

Virtualization for Unified CCE
Cisco Unified Contact Center Enterprise Design Guide

Software License Requirements

Cisco Products

The following table lists the Cisco components that comprise a Unified CCE solution:

<table>
<thead>
<tr>
<th>Components</th>
<th>License requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Contact Center Enterprise</td>
<td>One server license for each of: Voice applications, E-Mail Interaction Manager applications, and Web Interaction Manager applications. One agent license for each concurrent user with different feature tiers.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>One license for each Cisco Unified Communications Manager node, plus device licenses for connected devices.</td>
</tr>
<tr>
<td>Cisco Unified Customer Voice Portal</td>
<td>One Customer Voice Portal (CVP) software license for each server that runs Call Server or VXML Server software (or both coresident), ports or redundant ports, or Call Director software. One CVP reporting license for each Reporting Server. No license required for Operations Console. Port license package required for ports used for simultaneous sessions requiring self-service or queuing (voice and video). Redundant port licenses required for each redundant port. One license for each developer machine running Call Studio. Upgrade licenses from Unified IP IVR available.</td>
</tr>
<tr>
<td>Cisco Unified Intelligence Center</td>
<td>One license for each server.</td>
</tr>
</tbody>
</table>
### Components

<table>
<thead>
<tr>
<th>Components</th>
<th>License requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Finesse</td>
<td>Finesse: User licenses included with selected tiers of Cisco Unified Contact Center Enterprise user licenses. One license for each server pair. One license for each Media Kit.</td>
</tr>
<tr>
<td>or Cisco CTI OS</td>
<td></td>
</tr>
<tr>
<td>or CAD</td>
<td></td>
</tr>
<tr>
<td>Cisco Unified Contact Center Management Portal</td>
<td>User licenses included with selected tiers of Cisco Unified Contact Center Enterprise user licenses.</td>
</tr>
<tr>
<td>Cisco MediaSense</td>
<td>Server licenses required for Primary and Secondary Servers. Expansion Server Software licenses required for extra capacity. Session licenses (base, and either audio or video) required for each user.</td>
</tr>
<tr>
<td>Cisco SocialMiner</td>
<td>User license included with Unified CCE Premium Agent License. One server license for each SocialMiner server.</td>
</tr>
<tr>
<td>EIM/WIM</td>
<td>One agent license for each concurrent user with different feature tiers. One server license for each Email Interaction Manager and Web Interaction manager application.</td>
</tr>
</tbody>
</table>

#### Third-Party Products

The following table lists the third-party software products that work with Cisco components to comprise a Unified CCE solution.

<table>
<thead>
<tr>
<th>Software</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Server 2012 R2</td>
<td>For server applications</td>
</tr>
<tr>
<td>Microsoft SQL Server 2014</td>
<td>For applications that contain a database</td>
</tr>
<tr>
<td>Windows</td>
<td>For Administration Client applications</td>
</tr>
<tr>
<td>Antivirus</td>
<td>For all applications that run on the Windows platform</td>
</tr>
<tr>
<td>• Symantec Endpoint Protection</td>
<td></td>
</tr>
<tr>
<td>• Trend Micro Office Scan</td>
<td></td>
</tr>
<tr>
<td>• McAfee VirusScan Enterprise</td>
<td></td>
</tr>
</tbody>
</table>

**Note**


Before you begin an installation or upgrade of any part of your contact center, confirm the following:

- That you have all the required software products.
- That all the software versions are compatible with each other.
- That all software versions are also compatible with all hardware and VMware.

Related Topics

Compatibility Requirements, on page 7

Virtualization Requirements

You run the Unified Contact Center Enterprise solution on VMware ESXi platform. This solution requires that you run the virtualized machines (VMs) on Cisco Unified Computing System (UCS) B-series or C-series servers, or Third-party servers.

You install the Unified CCE components after you configure the VMs.

For detailed virtualization requirements, review Compatibility Requirements, on page 7 for VMware and Cisco software components.

In addition, the following requirements apply to VMware on virtual machines for Unified CCE:

- After you install the Unified CCE components on each VM, install the latest VMware Tools from your VMware host using the VMware Tool default settings. You require one license for VMware vSphere Standard or Enterprise ESXi for each host server.

  Note Update the VMware Tools whenever you patch or upgrade ESXi.

- If you experience slow mouse performance, see the following Knowledge Base item on the VMware website: Windows Display Driver Model.

Related Topics

Virtualization for Unified CCE
Install VMware Tools, on page 20
Compatibility Requirements

As part of the planning process, ensure that all hardware, Cisco software, third-party software, VMware, and firmware are compatible. Confirm that you meet all the following compatibility requirements:

<table>
<thead>
<tr>
<th>For this compatibility information</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware and Cisco software components</td>
<td>Unified Communications Virtualization Supported Applications at <a href="http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Supported_Applications">http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Supported_Applications</a></td>
</tr>
</tbody>
</table>
| Required firmware | See the following:  

**Note**  
Review the compatibility between different versions of the Cisco components to plan upgrades that occur across multiple maintenance windows. Components that are upgraded in one maintenance window must continue to operate with other components that are still at the previous version until the full upgrade is completed.
<table>
<thead>
<tr>
<th>For this compatibility information</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows OS and SNMP</td>
<td>See the following:</td>
</tr>
</tbody>
</table>
CHAPTER 2

Installation Overview

• Installation Tools, page 9
• Uninstallation, page 10

Installation Tools

During installation, use one or all of the following tools, as required:

• ICM-CCE-CCHInstaller—The main Unified CCE Installer copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE and Apache Tomcat. It uses the Microsoft .NET Framework which is an integral part of Windows Server 2012 R2.

  **Note** Optionally, you can update the JRE installed by the Unified CCE Installer with a later version of the JRE. See Update the Java Runtime Environment (Optional), on page 57.

You cannot run the installer remotely. Mount the installer ISO file only to a local machine.

  • Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.
  
  • Domain Manager—Used to provision Active Directory.
  
  • Web Setup—Used to set up the Call Routers, Loggers, and Administration & Data Servers.
  
  • Peripheral Gateway Setup—Used to set up PGs, the CTI server, and the Outbound Option dialer.

• AdminClientInstaller—Installs the Administration Client on a system that is not running other Unified CCE components.

The AdminClientInstaller is delivered on the installation media with the ICM-CCE-CCHInstaller.

• Administration Client Setup—Used to add, edit, or remove Administration Clients and Administration Client Instances.

The Administration Client Setup is delivered on the installation media with the ICM-CCE-CCHInstaller.
Uninstallation

Unified CCE supports the uninstall option from the Windows Add/Remove option. This option removes the patches, base version files, and the related registry. The option also removes Unified CCE component software installed by the ICM-CCE-CCHInstaller.

However, it does not remove the following:

- Java Runtime Environment
- Unified CCE databases

Reinstallation is also supported. To reinstall, rerun the ICM-CCE-CCHInstaller.
Preinstallation

- Preinstallation Task Flow, page 11
- Preinstallation Tasks, page 12

Preinstallation Task Flow

Before you can install Unified CCE and the associated components, set up the network, create virtual machines, and install and configure third-party software.

---

**Important**

After you set the hostname of any Unified CCE server, you cannot change it.

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you are integrating Unified CCE into an existing corporate network, verify Domain Controller health. If you are installing into a new Active Directory domain, install and configure Active Directory and DNS server.</td>
<td>Set up Active Directory, on page 12</td>
</tr>
<tr>
<td>Download Open Virtualization Format (OVA) templates and create virtual machines.</td>
<td>Set Up Virtual Machines, on page 16</td>
</tr>
<tr>
<td>Install and configure third-party software.</td>
<td>Set Up Third-Party Software, on page 18</td>
</tr>
</tbody>
</table>
Preinstallation Tasks

Set up Active Directory


Verify Domain Controller Health

Before you set up the Unified CCE DNS and Active Directory (AD) structure, ensure that your existing domain controller environment is stable. Install and run the following tools, available from the Microsoft Windows Server 2012 R2 installation media, in the Tools subfolder:

- `dcdiag.exe`—Generates a report on AD health, including connectivity, replication, topology integrity, intersite health, and trust verification. Checks Network Card (NC) head security descriptors, net logon rights, and roles. Locates the domain controller.

- `repadmin.exe`—Retrieves the replication status of all CSV > showrepl.csv domain controllers in a spreadsheet, verifies DNS infrastructure, Kerberos, Windows time service (W32time), remote procedure call (RPC), and network connectivity.

Ask your network administrator or qualified AD expert (for example, Microsoft Support Services) to evaluate the resulting reports from these tools.

Run `dcdiag.exe`

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Start &gt; Run.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Type <code>cmd</code>.</td>
</tr>
</tbody>
</table>
| Step 3 | Press **Enter**.  
A command console opens. |
| Step 4 | At the prompt, enter `dcdiag.exe /e /v /f:dcdiag.txt`.  
**Note**  
If you use the `/e` option, run `dcdiag.exe` at the root level. If you do not use the “/e” option, run `dcdiag.exe` on each individual domain controller.  
The application creates the text file `dcdiag.txt` in the folder containing `dcdiag.exe`. |
| Step 5 | Open the text file and note any items that are prefaced with “Warning” or “Error.” |
| Step 6 | Correct all the issues, then rerun `dcdiag.exe` to ensure that no issues remain. |
### Run repadmin.exe

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Choose <strong>Start &gt; Run</strong>.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Type <strong>cmd</strong>.</td>
</tr>
</tbody>
</table>
| **3** | Press **Enter**.  
  A command console opens. |
| **4** | At the prompt, enter `repadmin.exe /showrepl */csv > showrepl.csv`. |
| **5** | Open Excel and choose **File > Open**.  
  **Note**: Depending on your version of Excel, the menu cascades may be slightly different. |
| **6** | In the “Files of type” section, click **Text Files (*.prn;*.txt;*.csv)**. |
| **7** | In the “Look in” section, navigate to `showrepl.csv`, then click **Open**. |
| **8** | In the Excel spreadsheet, right-click the column heading for `showrepl_COLUMNS` (column A), then click **Hide**.  
  Select the row just under the column headings, then choose **Windows > Freeze Pane**. |
| **9** | Click the upper-left corner of the spreadsheet to highlight the entire spreadsheet. Choose **Data > Filter > AutoFilter**. |
| **10** | In the heading of the Last Success column, click the down arrow, then click **Sort Ascending**. |
| **11** | In the heading of the Source DC column, click the down arrow, then click **Custom**.  
  In the Custom AutoFilter dialog box, complete the custom filter as follows:  
  1. Under Source DC, click **does not contain**.  
  2. In the corresponding text box, enter del to filter deleted domain controllers from the spreadsheet. |
| **12** | In the heading of the Last Failure column, click the down arrow, then click **Custom**.  
  In the Custom AutoFilter dialog box, complete the custom filter as follows:  
  1. Under Last Failure, click **does not equal**.  
  2. In the corresponding text box, enter 0 to filter for only domain controllers that are experiencing failures. |
| **13** | Use **AutoFilter** in Excel to view the replication health for the following:  
  • Source replication partner  
  • The time that replication last occurred  
  • The time that the last replication failure occurred for each naming context (directory partition) |

For every domain controller in the forest, the spreadsheet shows the following:

- Source replication partner
- The time that replication last occurred
- The time that the last replication failure occurred for each naming context (directory partition)
You can observe the replication partners that replicate successfully.

**Step 16** Locate and resolve all errors.

**Step 17** Rerun repadmin.exe to ensure that no issues remain.

---

**Install DNS on Additional Domain Controller**

This topic is applicable only for Windows 2008 R2.

**Procedure**

**Step 1** Choose Start > Control Panel > Add/Remove Programs.

**Step 2** On the Add/Remove Windows Components, check Networking Services and click Details.

**Step 3** Check DNS, click OK, then select Next.

**Step 4** Browse to the Windows Server CD. DNS installation begins.

**Step 5** Validate that all DNS Zones were replicated from the first DNS Server in the AD Domain to this DNS Server.
   a) Select the machine name, right-click, and select Properties.
   b) On the Interfaces tab, select **Listen on only the following IP addresses**, remove all but the visible machine address.

---

**Configure Active Directory Sites**

Perform the following procedure on the Unified CCE root domain controller:

**Procedure**

**Step 1** Start > Programs > Administrative Tools > AD Sites and Services.

**Step 2** Rename the default first site name in accordance with your AD site plan.
   a) For a geographically separated Domain Controller, right-click Sites.
   b) Select New Site.
   c) Enter the site name of the additional domain controller based on your AD site plan.

**Step 3** Create subnets for each Domain Controller site:
   a) Right-click the Subnets folder and select New Subnet.
   b) Enter the subnet address and mask associated with the LAN at the Domain Controller Site.
   c) Highlight the Site Name that is associated with that subnet.

**Step 4** Expand the Servers folder from the original first site folder.

**Step 5** For each server that you must move to a different site, right-click the server name, select Move, and highlight the Site to which you want to move it.

**Step 6** Expand Inter-Site Transport under Sites.
a) Open the IP folder and select **DEFAULTIPSITELINK** from the right pane.
b) Right-click and select **Properties**. Ensure that both sites appear as entries in the Sites in this **Site Link** window.
c) Change the Replicate Every value to **15 minutes**.

**Assign Global Catalog and Set Time Source**

**Procedure**

**Step 1**
Open **Active Directory Sites and Services**.

**Step 2**
Connect to the Domain Controller that is designated as the Global Catalog.

**Step 3**
Right-click **NTDS Settings** and select **Properties**. Select **Global Catalog**.

**Step 4**
Move FS MO roles, according to your design plan.

The Forest Time Source defaults to the PDC Emulator, which is originally created on the Forest Root Domain Controller.

**Step 5**
If the PDC Emulator is on another Domain Controller, redefine the Time Source as either that server, or use an external Time Source.

a) On the server currently running the PDC Emulator, run the following command: `Net time /setsntp: <DNS Name of Time Source>`.

b) To synchronize a server to the Time Source, see the procedure available on the Microsoft website [http://support.microsoft.com/kb/816042](http://support.microsoft.com/kb/816042).

**Configure DNS Server on Forest Root Domain Controller**

**Procedure**

**Step 1**
Choose **Start > Programs > Administrative Tools > DNS**.

**Step 2**
Expand Hostname Tree.

**Step 3**
Expand Forward Lookup Zones.

**Step 4**
Select the machine name, then right-click and select **Properties**.

**Step 5**
On the Interfaces tab, select **Listen on only the following IP addresses** and remove all but the visible machine address.

**Step 6**
Configure AD Integrated Forward and Reverse Lookup Zones.

a) Select the Unified CCE Domain zone name under Forward Lookup Zones, right-click, and select **Properties**.

b) On the General tab, for Allow Dynamic Updates, select **Only Secure Updates** from the menu.

c) Use the Zone Transfers tab only when there is a trusted-site relationship between this domain and another domain. Transfer zone updates from this AD Integrated Zone to a Standard Secondary Zone on the DNS.
Servers in the other domain. Select **Allow Zone Transfers**, then select **only to the following servers** and enter the IP Addresses of the DNS Servers in the other domain.

Networks within a Forward Lookup Zone include all visible and private networks that are within a DNS Zone. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.

**Step 7** Under the Server Name, right-click **Reverse Lookup Zones** and select **New Zone**.

**Step 8** Within the New Zone wizard, select **Active Directory Integrated**.

**Step 9** In the Reverse Lookup Zone window, select **Network ID** and enter the required number of octets for the Reverse Lookup Zone. The Reverse Lookup Zone Name is automatically entered.

**Step 10** Repeat the following steps for each Unified CCE domain Reverse Lookup Zone:

a) Select the Zone name under Reverse Lookup Zones, then right-click and select **Properties**.

b) On the General tab, for Allow Dynamic Updates, select **Only Secure Updates** from the menu.

**Step 11** Manually complete the DNS Host and PTR records.

a) Manually enter the hostnames for the machines that house Unified CCE nodes, and all NICs and Peripherals for any Web Setup that requires hostname resolution, into the applicable DNS Forward Lookup Zone.

b) On the DNS Server, right-click on the **Forward lookup Zone Name** and select **New Host**. (The hostname of this Root Domain Controller is already in the file.)

c) Add all Unified CCE hostnames (visible, visible high, private, private high, SAN) and their associated IP addresses. Check the box to create an associated PTR Record (Reverse Lookup Zone record).

d) Manually enter any Peripherals (ACDs/VRUs) and NICs accessed by the Unified CCE using hostname resolution in the Forward Lookup Zone.

---

**Set Up Virtual Machines**

**Verify Datastores**

Before you install the VMs, verify that the datastore is in place. The type of datastore depends on the type of server on which you deploy the VMs. For example, UCS-B servers use a SAN datastore and UCS-C servers use DAS datastores.

For more information, see the *VMware documentation*.

**Download Unified CCE OVA Files**

The Unified CCE Open Virtualization Format (OVA) files define the basic structure of the corresponding VMs that are created. The structure definition includes the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

**Before You Begin**

You must have a valid service contract associated with your Cisco.com profile.
**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Go to the Unified CCE Download Software page on Cisco.com.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Download</strong> to download and save the appropriate OVA file to your local hard drive. When you create VMs, you select the OVA required for the application.</td>
</tr>
</tbody>
</table>

**Create Virtual Machines from OVA Files**

To create virtual machines (VMs) from the OVA files, complete the following procedure.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select the Host in the vSphere client.</td>
</tr>
<tr>
<td>2</td>
<td>Choose <strong>File &gt; Deploy OVF Template</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Browse to the location on your local drive where you stored the OVA. Click <strong>Open</strong> to select the file. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Next</strong> at the <strong>OVF Template Details</strong> page.</td>
</tr>
<tr>
<td>5</td>
<td>Enter the virtual machine name. It cannot contain spaces or special characters. Enter a maximum of 32 characters. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>6</td>
<td>On the <strong>Name and Location</strong> page, enter a name of your choice in the <strong>Name</strong> field. Click <strong>Next</strong>. <strong>Important</strong> After the VM is created, you cannot rename it.</td>
</tr>
<tr>
<td>7</td>
<td>On the <strong>Deployment Configuration</strong> page, select the applicable configuration from the drop-down list. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>8</td>
<td>Choose a data store on which to deploy the new virtual machine. Click <strong>Next</strong>. <strong>Note</strong> Some deployments require two data stores.</td>
</tr>
<tr>
<td>9</td>
<td>On the <strong>Disk Format</strong> page, choose <strong>Thick provisioned Eager Zeroed format</strong> for the virtual disk format. Click <strong>Next</strong>. <strong>Note</strong> <strong>Thick provisioned Lazy Zero</strong> is also supported, but <strong>Thin provisioned</strong> is not supported.</td>
</tr>
</tbody>
</table>
| 10   | Confirm that the **Network Mapping** page is correct:  
  a) Public network adapter to Public network  
  b) Private network adapter to Private network  
  **Note** For some deployments, only one network interface is available. |
| 11   | Click **Finish**. |
| 12   | At the Successfully Completed message, click **Close**. |
| 13   | In the vSphere Client, ensure that you have upgraded the VM hardware version to the latest version. For more information, see VMware Knowledge Base, *Upgrading a virtual machine to the latest hardware version (multiple versions)* (1010675). |
Mount and Unmount ISO Files

Upload ISO image to data store:
1. Select the host in the vSphere client and click **Configuration**. Then click **Storage** in the left panel.
2. Select the datastore that will hold the ISO file.
3. Right-click and select **Browse datastore**.
4. Click the **Upload** icon and select **Upload file**.
5. Browse to the location on your local drive where you saved the ISO file, and upload the ISO to the datastore.

Mount the ISO image:
1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Check **Connect at power on** (Device status panel upper right).
4. Click the Datastore ISO File radio button and then click **Browse**.
5. Navigate to the data store where you uploaded the file.
6. Select the ISO.

Unmount the ISO image:
1. Right-click the VM in the vSphere client and select **Edit virtual machine settings**.
2. Click **Hardware** and select **CD|DVD Drive 1**.
3. Uncheck **Connect at power on** (Device status panel, upper right).

Set Up Third-Party Software

Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server 2012 R2 on all virtual machines for server-based applications.

Procedure

Step 1 Mount the Microsoft Windows Server ISO image to the virtual machine. Check the **Connect at power on** checkbox when mounting the ISO.

For more information, see *Mount and Unmount ISO Files*, on page 18.

Step 2 Power on the VM.

Step 3 Enter the Language, Time and Currency Format, and Keyboard settings. Click **Next**.

Step 4 Click **Install Now**.

Step 5 Enter the product key for Windows Server 2012 R2 and click **Next**.

Step 6 Select **Windows Server 2012 R2 Standard (Server with a GUI)** and click **Next**.

Step 7 Accept the license terms and click **Next**.

Step 8 Select **Custom: Install Windows only (advanced)**, select **Drive 0** to install Microsoft Windows Server, and then click **Next**. The installation begins. After the installation is complete, the system restarts without prompting.

Step 9 Enter and confirm the password for the administrator account, and then click **Finish**.

Step 10 Enable Remote Desktop connections as follows:
   a) Navigate to **Control Panel > System and Security > System**.
   b) Click **Remote Settings**.
   c) Click the **Remote** tab.
   d) Select the **Allow remote connections to this computer** radio button, and click **OK**.

Step 11 Open the **Network and Sharing Center** and select **Local Area Connections**.

Step 12 In the **Network Settings** dialog box, configure the network settings and the Domain Name System (DNS) data:
   a) Select **Properties**. Uncheck **Internet Protocol Version 6 (TCP/IPv6)**.
   b) Select **Properties** again.
   c) Select **Use the following IP Address**.
   d) Enter the IP address, Subnet mask, and Default gateway and click **OK**.

Step 13 Navigate to **Control Panel > System and Security > System** and change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name cannot contain underscores or spaces.

You must restart for the change to take effect.

Step 14 Run Microsoft Windows Update.

After the update is complete, click **Do not enable automatic updates**.

Microsoft Windows Server 2012 R2 is installed. In addition, Internet Explorer 11 is installed automatically.

If Unified CCE language pack is applied on Chinese Windows machine, set the screen resolution to 1600 x 1200.

---

### Set Windows Locale

If the Windows system locale differs from the display language (and therefore also the SQL collation setting), some characters appear incorrectly in the user interface and are saved incorrectly to the database. For example, if the system locale is English and an agent works in Spanish, characters such as the acute accent do not appear correctly.

If you use a multilingual version of Microsoft Windows Server 2012 R2, complete this procedure to set the Windows locale.

**Procedure**

1. **Step 1** Open Control Panel, and click Clock, Language, and Region.
2. **Step 2** In the Region section, click Change date, time, or number formats.
3. **Step 3** Click the Administrative tab.
4. **Step 4** In the Language for non-Unicode programs section, click Change system locale.
5. **Step 5** In the Region Settings window, select the language that matches the display language.
6. **Step 6** Restart the virtual machine.

---

### Install VMware Tools

VMware Tools is a suite of utilities that enhance the performance of the virtual machine guest operating system and improve management of the virtual machine.

---

**Note**

If you are upgrading from Unified CCE Pre-11.0 Release version to Release 11.0 version, do not upgrade the VMware Tools (Version 4.x) prior to the product upgrade. If the VMware Tools upgrade is already done prior to the product upgrade, the network connectivity will be lost during the product upgrade and the upgrade will fail. The workaround for this issue is to update the vNIC from VMXNET3 to Flex and then begin the upgrade. As a side effect of this workaround, the upgrade will take longer than usual. Once the RU upgrade is completed, the vNIC can be updated back to VMXNET3.
### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Power on the virtual machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>When the Guest Operating Starts, prepare your virtual machine to install VMware tools.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose VM &gt; Guest &gt; Install VMware Tools.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Double-click your CD-ROM drive to open installation wizard. Click OK in the warning message.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose Typical option and click Next to begin installation.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Install.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click Finish.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Restart your system.</td>
</tr>
</tbody>
</table>

### Install Microsoft SQL Server

Install Microsoft SQL Server 2014, and store the SQL Server log and temporary files on the same physical disk as the operating system.

**Note**

**Before You Begin**

**Note**
If your computer has no internet connection to get the updates, you must download and install Microsoft .NET Framework 3.5 SP1 manually.

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Mount the Microsoft SQL Server ISO image to the virtual machine.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Run setup.exe.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Installation on the left pane and then click New SQL Server stand-alone installation or add features to an existing installation. Click OK.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Product Key page, enter the product key and then click Next.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Accept the License Terms and then click Next.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Optional: On the Microsoft Update page, check the Use Microsoft Update to check for updates check box, and then click Next.</td>
</tr>
</tbody>
</table>
If you do not check the **Use Microsoft Update to check for updates** check box, click **Next** on the **Product Updates** page.

**Step 7**  
On the **Install Rules** page, click **Next**.  
In this step, the installation program checks to see that your system meets the hardware and software requirements.

**Note**  
In case of any issues, warnings or errors are displayed. In the **Status** column, click the respective **Warning** or **Error** link for more information about a rule.

**Step 8**  
On the **Setup Role** page, select **SQL Server Feature Installation** and click **Next**.

**Step 9**  
On the **Feature Selection** page, select all the features except the following; and then click **Next**.

- Analysis Services
- Reporting Services-Native
- Reporting Services - SharePoint
- Reporting Services Add-in for SharePoint Products
- Distributed Replay Controller
- Distributed Replay Client

**Step 10**  
On the **Instance Configuration** page, select **Default Instance** and click **Next**.

**Step 11**  
On the **Server Configuration** page, click the **Services Account** tab.
In the Services Account tab, you must associate the SQL services with the virtual account.

- For the SQL Server Database Engine, in the Account Name field, select **NT Service\MSSQLSERVER**.
- For the SQL Server Agent service, in the Account Name field, select **NT Service\SQLSERVERAGENT**.

**Note**  
While you can use the Network or Local Services account instead of the Virtual account, using the Virtual account provides better security.

**Step 12**  
For the remaining services, accept the default values.

**Step 13**  
In the **Start Up Type** column, for the **SQL Server Agent service** account, select **Automatic** from the list.

**Step 14**  
On the **Server Configuration** page, select the **Collation** tab.

a) In the Database Engine section, click **Customize**.

b) Select the **Windows Collation designator and sort order** radio button.

c) Select the appropriate collation. Typically, you should choose the SQL Server collation that supports the Windows system locale most commonly used by your organization; for example, "Latin1_General" for English.

**Note**  
Refer to the **Unified CCE Solution Compatibility Matrix** at [http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE](http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE) for details about collations used for other languages. The collation you select affects what is written to the database. For example, if you set the collation for Latin1_General and a user at the customer site selects Chinese as the language selection at sign-in and enters field values in Chinese, the application returns an unsupported characters error because the database is unable to save the characters.

**Important**  
It is critical to select the correct collation setting for the customer's language display. If you do not select the correct collation during installation, the customer must uninstall and re-install Microsoft SQL Server.

d) Check the **Binary** check box.
e) Click OK, and then click Next.

**Step 15** On the Database Engine Configuration page:
- a) On the Server Configuration tab, click the Mixed Mode radio button.
- b) Enter the password for the SQL Server system administrator account, and confirm by reentering it.
- c) Click Add Current User to add the user who is installing the SQL Server as an administrator.
- d) Click Next.

**Step 16** On the Ready to Install page, click Install.

**Step 17** On the Complete page, click Close.

**Step 18** Enable Named Pipes and set the sort order as follows:
- a) Open the SQL Server 2014 Configuration Manager.
- b) In the left pane, navigate to SQL Native Client 11.0 Configuration (32bit) > Client Protocols.
- c) In the right pane, right-click Named Pipes and confirm that Enable is selected.
- d) In the Client Protocols Properties window, select Named Pipes and click Move Up or Move down to change the order of the protocols as follows: Shared Memory, Named Pipes, TCP/IP, and then click OK.
- e) In the left pane, navigate to SQL Server Network Configuration > Protocols for MSSQLSERVER.
- f) In the right pane, right-click Named Pipes and select Enable.

**Step 19** Set the SQL Server's default language to English as follows:
- a) From the SQL Server Management Studio, right-click the server and select Properties.
- b) Click Advanced.
- c) In the Miscellaneous section, set the Default Language to English.
- d) Click OK.

**Important** You must set the SQL Server default language to English because Unified CCE requires a US date format (MDY). Many European languages use the European date format (DMY) instead. This mismatch causes queries such as

```
SELECT * FROM table WHERE date = '2012-04-08 00:00:00'
```

to return data for the wrong date. Handle localization in the client application, such as Cisco Unified Intelligence Center.

**Step 20** Restart the SQL Server service as follow:
- a) Navigate to the Windows Services tool.
- b) Right-click SQL Server (MSSQLSERVER) and click Stop.
- c) Right-click SQL Server (MSSQLSERVER) and click Start.

**Step 21** Ensure that the SQL Server Browser is started, as follows:
- a) Navigate to the Windows Services tool.
- b) Navigate to the SQL Server Browser.
- c) Right-click to open the Properties window.
- d) Enable the service and change the startup type to Automatic.

---

**What to Do Next**

The SQL Server installation disables the Windows Computer Browser service. The ICMDBA requires this service. If you need to run ICMDBA on this server, enable the Computer Browser service.
Set Users as System Administrators

Any users who are involved in installing or upgrading a Unified ICM/CCE solution must be added as part of SQL Server Security login and associated with the System Administrator role. To set a user as a System Administrator, complete the following steps.

Procedure

**Step 1** Open the SQL Server Management Studio using the System Administrator login credentials.

**Step 2** In the Object Explorer pane, click the **Security** folder.

The **Security** folder expands.

**Step 3** Right-click the **Logins** folder, and then click **New Login**.

The Login-New view appears.

**Step 4** In the Login name field, enter the Windows login name of the user whom you want to associate with the System Administrator role.

**Step 5** Click **OK**.

**Step 6** In the Object Explorer pane, click the **Server Roles** folder.

The Server Roles view appears.

**Step 7** Check the **sysadmin** check box.

**Step 8** Click **OK**.

The user is now a part of the SQL Security login and is also associated with the System Administrator role.

Install Antivirus Software

All VMs in your contact center require antivirus software. Unified CCE supports the following antivirus products:

- McAfee VirusScan
- Symantec Endpoint Protection
- Trend Micro Server Protect Version


Use your antivirus vendor's product documentation for installation instructions, and adhere to the following:

- Update antivirus software manually. Do not enable automatic updates.
- To allow required access to installation program files or folders, perform file-blocking exclusions in the antivirus product file-and-folder protection rules. For example, to create the exclusions in McAfee VirusScan:
  1. Open the VirusScan console.
  2. Right-click **Access Protection** and select **Properties**.
3 In the Anti-virus Standard Protection category, make sure that the rule **Prevent IRC communication** is unchecked in the **Block** column.

- Be aware that in the firewall component of Symantec Endpoint Protection 12.1, the Network Threat Protection feature must be disabled. The feature is enabled by default. When the feature is enabled, both sides of a redundant router come up in stand-alone mode which blocks communication between each side of the router pair. This blocking affects all deployment types.

If you retain the default (enabled) and start services on side A and B of the router, the following Symantec message appears in the system tray: “The client will block traffic from IP address [side A router address] for the next 600 seconds.” The same message is also written to the security login client management. The Symantec Network Threat Protection traffic log indicates that a default firewall rule called “Block_all” was dynamically enabled. The router logs show that both sides of the router came up in stand-alone mode.

To resolve the issue, disable the Symantec firewall and restart both sides of the router pair:

1 Double-click the Symantec icon in the system tray and select **Change Settings**.

2 Configure settings for **Network Threat Protection** and uncheck the **Enable Firewall** check box at the top of the **Firewall** tab.

**Configure a Database Drive**

Complete the following procedure for virtual machines that require another hard drive to archive data.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><strong>Start &gt; All Programs &gt; Administrative Tools &gt; Computer Management.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>In the left pane, expand <strong>Storage</strong> and click <strong>Disk Management</strong></td>
</tr>
<tr>
<td>Step 3</td>
<td>On the <strong>Disk Management</strong> window, in the left pane, right-click <strong>Disk 1</strong>, and then select <strong>Online</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Right-click <strong>Disk 1</strong> again, and select <strong>Initialize Desk</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the <strong>Initialize Desk</strong> window, for the Use the following partition style for the selected disks: option, choose the <strong>MBR (Master Boot Record)</strong> radio button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>To create a new disk partition, right-click the right pane corresponding to <strong>Disk 1</strong> and select <strong>New Simple Volume</strong>.</td>
</tr>
</tbody>
</table>
| Step 7 | In the **New Simple Volume Wizard** window, ensure that the **Format this volume with the following settings**: option is selected.  
  a) Retain the default file system (NTFS).  
  b) Retain the default allocation unit size.  
  c) Enter a name for the Volume label.  
  d) Check the **Perform a quick format** check box.  
  e) Click **Next**.  
  f) Click **Finish**.  
  The format is complete when the status changes to Healthy. |

The SQL reporting data is stored on this disk.
CHAPTER 4

Installation

• Installation Task Flow, page 27
• Installation Tasks, page 29
• Update the Java Runtime Environment (Optional), page 57
• Silent installation, page 57
• Cisco Finesse Server Installation, page 58

Installation Task Flow

This section lists the installation tasks for a Unified CCE contact center solution.

Installation procedures for Unified CCE components appear later in this chapter. For the non-Unified CCE components in your solution, follow the links in the table to access the installation guides for those components.

For the Unified CCE components, the sequence you follow can vary according to the distribution of Unified CCE components on virtual machines.

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure that virtual machines are ready for installation</td>
<td>Set Up Virtual Machines for Installation, on page 30</td>
</tr>
<tr>
<td>Install Unified Communications Manager</td>
<td>Installing Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>Install Unified CCE components (Router, Logger, Administration &amp; Data Servers, peripherals)</td>
<td>Install Unified CCE Component Software, on page 38</td>
</tr>
<tr>
<td>Install Outbound Option</td>
<td>Create Outbound Option Database, on page 42 and then see</td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
</tr>
</tbody>
</table>
| Install Finesse  
or  
Install CTI OS Server  
or  
Cisco Agent Desktop Server  
Note The CTI Toolkit Desktop and Cisco Agent Desktop are deprecated in Unified CCE Release 11.0(1). Do not include these desktops in new deployments. Support for these desktops will be removed in a future release. | Cisco Finesse Server Installation, on page 58  
or  
or  
| (If deployment does not use Finesse)  
Install CTI OS Agent Desktops  
or  
Install Cisco Agent Desktops  
Note The CTI Toolkit Desktop and Cisco Agent Desktop are deprecated in Unified CCE Release 11.0(1). Do not include these desktops in new deployments. Support for these desktops will be removed in a future release. | CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise at http://www.cisco.com/en/US/products/sw/custcosw/ps14/prod_installation_guides_list.html  
or  
| Install Live Data | Live Data Installation, on page 32 |
### Installation Tasks

The following section provides instructions about installing Unified CCE components. For instructions about installing non-Unified CCE components in a Unified CCE solution, see the links to component-specific documents in the Installation Task Flow, on page 27.

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
</table>

1. If you are using IP IVR for self-service and queueing, see Getting Started with Cisco Unified IP IVR.

---

*Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, Release 11.0(1)***
Set Up Virtual Machines for Installation

Validate Network Adapter Settings and Power On

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select the virtual machine (VM) in the vSphere client. Right-click the VM and choose <strong>Edit settings</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Hardware tab, select each network adapter. Make sure that <strong>Connect at power on</strong> in the Device Status group is checked.</td>
</tr>
</tbody>
</table>
| Step 3 | Under Network Connection, select the applicable network connection from the **Network label** drop-down list:  
- Network adapter 1 = **Public**  
- Network adapter 2 = **Private**  
  **Note** Certain VMs do not require a private network connection. The OVAs for those VMs do not create a second network adapter. |
| Step 4 | Close the dialog box. |
| Step 5 | If you are powering up the VM for the first time, power on the VM and wait for the VM to restart and to apply customization. The restart can take 5–10 minutes.  
  **Important** Do not press Ctrl-Alt-Delete. If you press Ctrl-Alt-Delete after powering on, the customization does not take effect, which requires completing the customization manually. For more information, see the Docwiki page on this topic at [http://docwiki.cisco.com/wiki/Recover_from_Pressing_Ctrl-Alt-Del_During_Power-On](http://docwiki.cisco.com/wiki/Recover_from_Pressing_Ctrl-Alt-Del_During_Power-On). |

Configure Network Cards

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the vSphere client, select <strong>Start</strong>, right-click <strong>Network</strong>, and select <strong>Properties</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Change adapter settings</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Rename the Local Area Connection to <strong>visible</strong> for the Public network card.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Rename the Local Area Connection 2 to <strong>private</strong> for the Private network card.</td>
</tr>
<tr>
<td>Step 5</td>
<td>On the Network Connections page, press <strong>Alt-F</strong> to display the Advanced menu.</td>
</tr>
<tr>
<td>Step 6</td>
<td>From the Advanced menu, select <strong>Advanced Settings</strong>.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Under Adapters and Bindings, sort the connections so that <strong>visible</strong> is on top, and click <strong>OK</strong>.</td>
</tr>
</tbody>
</table>
Configure Private Ethernet Card

Procedure

| Step 1 | Right-click private and select Properties. |
| Step 2 | Uncheck Client for Microsoft Networks. |
| Step 3 | Uncheck File and Printer Sharing for Microsoft Networks. |
| Step 4 | Uncheck Internet Protocol Version 6 (TCP/IPV6). |
| Step 5 | Check Internet Protocol Version 4 (TCP/IPV4) and click Properties. |
|         | a) Remove the IP Address for the Default Gateway. |
|         | b) Remove the IP Address for the Preferred DNS server. |
|         | c) Remove the IP Address for the Alternate DNS server. |
| Step 6 | Click the Advanced button. Open the DNS tab. Uncheck Register this connection's addresses in DNS. |
| Step 7 | Add an entry for the private IP address. Append a suffix such as p to the hostname for this IP, to identify it as private. |
| Step 8 | Optional: Add another entry for the public high IP address. Append a suffix such as ph to the hostname for this IP, to identify it as public high. |
| Step 9 | Click OK twice. Then, click Close. |

Configure Visible Ethernet Card

Procedure

| Step 1 | Right-click public and select Properties. |
| Step 2 | Check Client for Microsoft Networks. |
| Step 3 | Check File and Printer Sharing for Microsoft Networks. |
| Step 4 | Uncheck Internet Protocol Version 6 (TCP/IPV6). |
| Step 5 | Check Internet Protocol Version 4 (TCP/IPV4) and click Properties. |
| Step 6 | Confirm the Public IP address, Subnet mask, Default gateway and Preferred DNS server, and click Advanced. |
| Step 7 | On the Advanced tab, enter the high public addresses. |
| Step 8 | On the DNS tab, in the DNS suffix for this connection field, enter the name of the local DNS zone for the server and check Register this connection's addresses in DNS. |
| Step 9 | Optional: Add another entry for the public high IP address. Assign an unique suffix, for example, ph to the hostname for this IP, to identify it as public high. |
| Step 10 | If the server requires access to resources in a different trusting or trusted domain or DNS zone, select Append these DNS suffixes (in order) and enter the local DNS zone for the server first, and then add the other secondary zones that represent the trusting or trusted domain. |
Live Data Installation

Follow this sequence of tasks to install Live Data.

You deploy Live Data on its own VM. Deploying Live Data co-resident with CUIC on a single VM is not a supported deployment for UCCE 11.0

Note: You deploy Live Data on its own VM. Deploying Live Data co-resident with CUIC on a single VM is not a supported deployment for UCCE 11.0.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set Deployment Type, on page 37</td>
</tr>
<tr>
<td>2</td>
<td>Check that you have created a separate virtual machine for the Live Data primary node and the Live Data secondary node. See Set Up Virtual Machines, on page 16.</td>
</tr>
<tr>
<td>3</td>
<td>Install Live Data Primary Node, on page 32</td>
</tr>
<tr>
<td>4</td>
<td>Set Live Data Secondary Node, on page 33</td>
</tr>
<tr>
<td>5</td>
<td>Install Live Data Secondary Node, on page 34</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade VMware Tools, on page 35</td>
</tr>
<tr>
<td>7</td>
<td>Configure Live Data with AW, on page 35</td>
</tr>
<tr>
<td>8</td>
<td>Configure Live Data Machine Services, on page 36</td>
</tr>
<tr>
<td>9</td>
<td>Configure Live Data Unified Intelligence Center Data Sources, on page 37</td>
</tr>
<tr>
<td>10</td>
<td>Restart Live Data</td>
</tr>
<tr>
<td>11</td>
<td>Set up Certificates for Live Data, on page 245</td>
</tr>
</tbody>
</table>

Install Live Data Primary Node

Procedure

Step 1 Mount the ISO image for the software to the virtual machine.
Step 2 Select the virtual machine and power it on.
Step 3 Follow the Install wizard, making selections as follows:
   a) In the Disk Found screen, click Yes to begin the verification of the media integrity.
   b) In the Success screen, select OK.
   c) In the Product Deployment Selection screen, select Live Data, and then select OK.
   d) In the Proceed with Install screen, select Yes.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.
i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, select **Yes**.

n) Enter your DNS Client Configuration. Select **OK**.
o) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
p) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.

q) In the **First Node Configuration** screen, select **Yes**.
r) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
s) In the **Security Configuration** screen, enter the security password and select **OK**.
t) In the **SMTP Host Configuration** screen, select **No**.
u) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
w) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and can run unattended.

- There is a reboot in the middle of the installation.
- The installation ends at a sign-in prompt.

**Step 4** Unmount the ISO image.

---

**Set Live Data Secondary Node**

You must provide the primary node the address of the secondary node. You do this with the `set live-data secondary` command.

**Procedure**

**Step 1** Log in to your primary Live Data node.

**Step 2** Run the following command to set the secondary node:

```
set live-data secondary name
```
Install Live Data Secondary Node

Before You Begin

Procedure

**Step 1** Mount the ISO image for the software to the virtual machine.

**Step 2** Select the virtual machine and power it on.

**Step 3** Follow the Install wizard, making selections as follows:

a) In the Disk Found screen, click Yes to begin the verification of the media integrity.

b) In the Success screen, select OK.

c) In the Product Deployment Selection screen, select Live Data, and then select OK.

d) In the Proceed with Install screen, select Yes.

e) In the Platform Installation Wizard screen, select Proceed.

f) In the Apply Patch screen, select No.

g) In the Basic Install screen, select Continue.

h) In the Timezone Configuration screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select OK.

i) In the Auto Negotiation Configuration screen, select Continue.

j) In the MTU Configuration screen, select No to keep the default setting for Maximum Transmission Units.

k) In the DHCP Configuration screen, select No.

l) In the Static Network Configuration screen, enter static configuration values. Select OK.

m) In the DNS Client Configuration screen, select Yes.

n) Enter your DNS Client Configuration. Select OK.

o) In the Administrator Login Configuration screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select OK.

p) In the Certificate Information screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select OK.

q) In the First Node Configuration screen, select No.

r) In the warning screen, select OK.

s) In the Network Connectivity Test Configuration screen, select No.

t) In the First Node Access Configuration screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select OK.

u) In the SMTP Host Configuration screen, select No.

v) In the Platform Configuration Confirmation screen, select OK. The installation begins and can run unattended.

- There is a reboot in the middle of the installation.

- The installation ends at a sign-in prompt.
Step 4  Unmount the ISO image.

Upgrade VMware Tools

To ensure that your version of the VMware Tools is current, refresh the installed version of VMware Tools from the local VMware host on both Live Data nodes.

Procedure

Step 1  Log in to the primary Live Data node.
Step 2  Run the command to update the VMware Tools: `utils vmtools refresh`
Step 3  Log in to the secondary Live Data node.
Step 4  Run the command to update the VMware Tools: `utils vmtools refresh`

Configure Live Data with AW

This command tells Live Data how to access the primary AW DB and the secondary AW DB. The command also automatically tests the connection from Live Data to the primary or secondary AW, checks to see if the configured user has appropriate AW DB access, and reports the results.

You can use the optional skip-test parameter if you do not want the test performed. When you include the skip-test parameter, no checking is done to see if the configured user has appropriate AW DB access, and no results are reported.

Before You Begin

Before you can configure Live Data, you must first configure a SQL user (with special permissions) to work with Live Data, as described in Configure SQL User Account, on page 113.

The SQL administrative user "sa" or a user with sysadmin privileges must then execute the following SQL queries for the SQL user configured to work with Live Data.

```sql
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "<user>"
GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "<user>"
```

Procedure

Step 1  Log in to your Live Data server.
Step 2  Run the following command to configure Live Data with the primary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results. (The skip-test parameter is optional; include it only if you do not want the test performed.)

```
set live-data aw-access primary addr port db user pwd [ skip-test ]
```
Step 3  Run the following command to configure Live Data with the secondary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results. (The skip-test parameter is optional; include it only if you do not want the test performed.)

```
set live-data aw-access secondary addr port db user pwd [ skip-test ]
```

You can also optionally run the following command at any time to show and test the AW configuration that you set from Live Data to the primary and secondary AW DBs. (The skip-test parameter is optional; include it only if you do not want the test performed.)

```
show live-data aw-access [ skip-test ]
```

Related Topics

- set live-data aw-access, on page 238
- show live-data aw-access, on page 239
- Configure SQL User Account, on page 113

Configure Live Data Machine Services

This command tells the AW where your Live Data machine services are located.

Procedure

**Step 1**  Log in to your Live Data server.

**Step 2**  Run the following command to configure the Live Data machine services:

```
set live-data machine-services awdb-user awdb-pwd
```

Use the `user@domain` format to specify the AW database domain user with write-access permission. The domain is a fully qualified domain name (FQDN), and the username is a user principal name. You must be authorized to change Unified CCE configuration.

**Note**

- The Machine Services table is autopopulated with the Router and Peripheral Gateway (PG) TIP connection information. This enables the Live Data server to establish a connection, and receive agent and call events as they occur.

  The connection information is autopopulated only if your deployment supports Live Data. To set the deployment type, see Set Deployment Type, on page 37.

- Currently, only Cisco Unified Communications Manager (CUCM) type PG and generic PGs with CUCM peripherals are supported for Live Data.

Related Topics

- set live-data machine-services, on page 244
Configure Live Data Unified Intelligence Center Data Sources

This command tells Unified Intelligence Center how to access Live Data.

Procedure

Step 1  Log in to your Live Data server.
Step 2  Run the following command to configure your Live Data Unified Intelligence Center data sources:

```
set live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd
```

Related Topics

set live-data cuic-datasource, on page 242

Set Deployment Type

Before you install or upgrade Live Data you must set the deployment type.

Note

You can use Live Data only on the following deployment types: UCCE 8000 Agents Router/Logger, UCCE 12000 Agents Router/Logger, and UCCE 4000 Agents Logger.

Procedure

Step 1  Navigate to Unified CCE Administration > System > Deployment.
Step 2  Select your deployment from the drop-down menu and click Next.

Set Up Certificates for Live Data

If you use HTTPS for secure Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, you must set up security certificates. For the Finesse and Cisco Unified Intelligence Center servers to communicate with the Live Data server, you must import the Live Data certificates and Cisco Unified Intelligence Center certificates into Finesse, and the Live Data certificates into Cisco Unified Intelligence Center.

For complete information, see Certificates for Live Data, on page 245.
Install Unified CCE Component Software

**Procedure**

**Step 1** Mount the Unified CCE Installer ISO image to the virtual machine. For more information, see Mount and Unmount ISO Files, on page 18.

**Step 2** Open the ICM-CCE-CCHInstaller and click Next.

**Step 3** Select **Fresh Install** and click **Next**.

The installer program proceeds through a series of screens on which you specify information.

Note: If you are installing a Unified CCE Logger and intend to deploy Outbound Option, select the **Enable Outbound Option** box as you progress through the Add Logger screens.

Note: Select the **Syslog** box to enable Syslog service.

**Step 4** Reboot the server when the installation is complete.

Set up Organizational Units

**Add a Domain**

Use the Domain Manager tool to add a domain.

**Procedure**

**Step 1** Open the Domain Manager tool and under Domains, click **Select**.

**Step 2** You can add domains through the Select Domains dialog box, or you can add a domain manually if the target domain cannot be detected automatically.

To add domains by using the controls in the Select Domains dialog box:

a) In the left pane under Choose domains, select one or more domains.

b) Click **Add** to add the selected domains, or click **Add All** to add all the domains.

To add a domain manually:

a) In the field under Enter domain name, enter the fully qualified domain name to add.

b) Click **Add**.

c) Click **OK**.

Add Organizational Units

Use the Domain Manager tool to create the Cisco root Organizational Unit (OU) for a domain, and then create the facility and instance OUs.
The system software always uses the root OU named Cisco_ICM. You can place the Cisco_ICM OU at any level within the domain where the Unified ICM Central Controller is installed. The system software components locate the root OU by searching for this name.

The user who creates the Cisco Root OU automatically becomes a member of the Setup Security Group for the Cisco Root OU. In effect, this user is granted privileges to all Unified CCE tasks in the domain.

**Procedure**

**Step 1**  
Open the Domain Manager tool and log in to an administrator account in the domain.

**Step 2**  
Choose the domain.

**Step 3**  
If this OU is the first instance, add the Cisco_ICM root:  
   a) Under Cisco root, click **Add**.  
   b) Select the OU under which you want to create the Cisco root OU, then click **OK**.  
      When you return to the Domain Manager dialog box, the Cisco root OU appears either at the domain root or under the OU you selected. You can now add the facility.

**Step 4**  
Add the facility OU:  
   a) Select the Cisco Root OU under which you want to create the facility OU.  
   b) In the right pane, under Facility, click **Add**.  
   c) Enter the name for the Facility, and click **OK**.

**Step 5**  
Add the instance OU:  
   a) Navigate to and select the facility OU under which you want to create the instance OU.  
   b) In the right pane, under Instance, click **Add**.  
   c) Enter the instance name and click **OK**.

**Step 6**  
Click **Close**.

**Add Users to Security Groups**

To add a domain user to a security group, use this procedure. The user is then granted the user privileges to the functions that are controlled by that security group.
Procedure

Step 1 Open the Domain Manager tool and select the Security Group you want to add a user to.
Step 2 Under Security group, click Members.
Step 3 Under Users, click Add.
Step 4 Select the domain of the user you want to add.
Step 5 (Optional) In the Optional Filter field, choose to further filter by the Name or User Logon Name, apply the search condition, and enter the search value.
Step 6 Click Search.
Step 7 Select the member you want to add to the Security Group from the search results.
Step 8 Click OK.

Set Up Unified CCE Central Controller Components

Add Unified CCE Instance

Procedure

Step 1 Open the Unified CCE Web Setup tool.
Step 2 Sign in as a domain user with local Administrator rights.
Step 3 Click Instance Management, and then click Add.
Step 4 On the Add Instance page, from the drop-down list, choose the customer facility and instance.
Step 5 Enter an instance number.
   The same instance name can occur more than once in a domain, so the instance number provides the uniqueness. The instance number must be between 0 and 24. The instance number must match for the same instance across your entire deployment. For an Enterprise (single instance) deployment, select 0 unless there are reasons to select another value.
Step 6 Click Save.

Create Component Databases

To improve database performance, ICM uses a reduced fill factor from previous releases for the index pages in every table of the Logger, AW, and HDS databases.

Create Logger Database

Perform this procedure on the Side A and Side B Loggers.
Procedure

Step 1 Open the ICMDBA tool, and click Yes at any warnings that display.
Step 2 Navigate to Server > Instance.
Step 3 Right-click the instance name and choose Create to create the logger database.
Step 4 In the Select Component dialog box, choose the logger you are working on (Logger A or Logger B). Click OK.
Step 5 At the prompt, “SQL Server is not configured properly. Do you want to configure it now?”, click Yes.
Step 6 On the Configure page, in the SQL Server Configurations pane check Memory (MB) and Recovery Interval. Click OK.
Step 7 On the Stop Server page, click Yes to stop the services.
Step 8 In the Select Logger Type dialog box, choose Enterprise. Click OK to open the Create Database dialog box.
Step 9 Create the Logger database and log as follows:
   a) In the DB Type field, choose the Side (A or B).
   b) In the region field, choose your region.
   c) In the Storage pane, click Add.
   d) In the Create Database dialog box, click Add to open the Add Device dialog box.
   e) Click Data.
   f) Choose the drive on which you want to create the database, for example, the E drive.
   g) For the Size field, consider whether to choose the default (which is 1.4GB, a fairly minimal size) or calculate a value appropriate for your deployment by using the Database Size Estimator Tool. If you calculate the value, enter it here.
   h) Click OK to return to the Create Database dialog box.
   i) Click Add again.
   j) In the Add Device dialog box, click Log.
   k) Choose the drive where you created the database.
   l) In the Size field, choose the default setting or, if you calculated an appropriate size for your deployment, enter that value.
   m) Click OK to return to the Create Database dialog box.
Step 10 In the Create Database dialog box, click Create, then click Start.
Step 11 When you see the successful creation message, click OK and then Close.

Create HDS Database

Perform this procedure on the Administration & Data Server on which you want to create the HDS database.
Procedure

Step 1  Open the ICMDBA tool, and click Yes at any warnings that display.
Step 2  Navigate to Servers > Instances.
Step 3  Right-click the instance name and choose Create.
Step 4  In the Select Component dialog box, choose Administration & Data Server. Click OK.
Step 5  At the prompt “SQL Server is not configured properly. Do you want to configure it now?”, click Yes.
Step 6  On the Configure dialog box, click OK.
Step 7  On the Select AW Type dialog box, choose Enterprise. Click OK to open the Create Database dialog box.
Step 8  Create the HDS database as follows:
   a) From the DB Type drop-down list, choose HDS.
   b) Click Add.
   c) On the Add Device dialog box, select Data.
   d) From the Available Drives list, choose the drive on which you want to install the database.
   e) In the Size field, you can leave the default value or enter an appropriate size for your deployment.
      Note  You can use the Database Size Estimator Tool to calculate the appropriate size for your deployment.
    f) Click OK to return to the Create Database dialog box.
   g) Click Add.
   h) On the Add Device dialog box, select Log.
   i) From the Available Drives list, choose the drive on which you created the database.
   j) In the Size field, you can leave the default value or enter an appropriate size for your deployment.
   k) Click OK to return to the Create Database dialog box.
Step 9  On the Create Database dialog box, click Create and then click Start.
Step 10  When you see the successful creation message, click OK and then click Close.

Create Outbound Option Database

Outbound Option uses its own SQL database on the Logger. Perform the following procedure on the Side A Logger only.

**Procedure**

**Step 1** Open the ICMDBA tool and click Yes to any warnings.

**Step 2** Navigate to Servers > <Logger Server> > Instances > <Unified CCE instance> > LoggerA. Right-click the instance name and select Database > Create.

**Step 3** On the Stop Server message, click Yes to stop the services.

**Step 4** In the Create Database dialog box, click Add to open the Add Device dialog box. Click Data, and choose the E drive. Leave the DB size with default value and click OK to return to the Create Database dialog box.

**Step 5** In the Add Device dialog box, click Log. Choose the desired drive. Leave the log size field with default value, and click OK to return to the Create Database dialog box.

**Step 6** In the Create Database dialog box, click Create, and then click Start. When you see the successful creation message, click OK and then click Close.

---

**Add Components to Unified CCE Instance**

**Add Logger Component to Instance**

Perform this procedure on the Side A and Side B Loggers.

**Procedure**

**Step 1** Open the Web Setup tool.

**Step 2** Choose Component Management > Loggers. Click Add, and then choose the instance.

**Step 3** On the Deployment page, select the Logger (A or B). Click Duplexed, and then click Next.

**Step 4** On the Central Controller Connectivity page, enter the host names for Sides A and B for the Router Private Interface and Logger Private Interface. Then, click Next.

**Step 5** On the Additional Options page, click Display Database Purge Configuration Steps.

**Step 6** Select the Enable Outbound Option box if you are installing a Unified CCE Logger and intend to deploy Outbound Option.

**Step 7** Select the Syslog box to enable the Syslog event feed process (cw2kfeed.exe).


**Step 8** If an external AW-HDS-DDS exists in the deployment, check Enable Historical/Detail Data Replication. If no external AW-HDS-DDS exists in the deployment, leave Enable Historical/Detail Data Replication unchecked.

**Step 9** Check Display Database Purge Configuration Step, and click Next.

**Step 10** On the Data Retention page, modify the Database Retention Configuration table:

a) For these tables, set the retention period to 40 days:
Add Router Component to Instance

Perform this procedure for Side A and Side B Routers.

Procedure

Step 1 In the Web Setup tool, select Component Management > Routers.
Step 2 Click Add to set up the Call Router.
Step 3 In the Deployment dialog, select the appropriate side.
Step 4 Click Duplexed, and then click Next.
Step 5 In the Router Connectivity dialog, configure the Private Interface and Public (Visible) Interfaces. Click Next.
Step 6 In the Enable Peripheral Gateways dialog, enter 1-2 in the Enable Peripheral Gateways field. Click Next.
Step 7 In the Router Options dialog, the Enable Quality of Service (QoS) is enabled by default. Click Next. Keep QoS enabled for all Unified CCE Private network traffic. For most deployments, disable QoS for the Visible (public) network traffic. For more details, refer to the appropriate section in the Cisco Unified Contact Center Enterprise Design Guide at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.
Step 8 In the Router Quality of Service dialog, click Next.
Step 9 In the Summary dialog, make sure that the Router summary is correct, then click Finish.
Add Administration & Data Server Component to Instance

Follow this procedure for all types of Administration & Data Servers:

- **Configuration-Only Administration Server**—Supports configuration changes only. Does not support reporting.
- **Administration Server and Realtime Data Server (AW)**—Supports configuration changes and real-time reporting. Does not support historical reporting.
- **Administration Server, Realtime and Historical Data Server, and Detail Data Server (AW-HDS-DDS)**—Supports configuration and real-time and historical reporting, including call detail and call variable data.

Not all fields apply to all server types.

**Note**

Data from the Config_Message_Log table is replicated from the Logger database to the AW database; you can use the AW database for auditing purposes. When you add the Administration & Data Server component, the retention period for the Config_Message_Log table in the AW database defaults of 90 days. To change the retention period, modify the following registry key:

```
Cisco Systems, Inc.\ICM\<instancename>\Distributor \RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog.
```

**Procedure**

**Step 1**
Open the Web Setup tool.

**Step 2**
Select **Component Management > Administration & Data Servers**. Click **Add**.

**Step 3**
On the Deployment page, choose the current instance.

**Step 4**
On the Add Administration & Data Servers page, configure as follows:

- **a)** Click **Enterprise**.
- **b)** Select the deployment size:

<table>
<thead>
<tr>
<th>Administration &amp; Data Server type</th>
<th>Choose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Server and Real-Time Data Server (AW)</td>
<td><strong>Small to Medium Deployment Size</strong></td>
</tr>
<tr>
<td>Configuration-Only Administration Server</td>
<td></td>
</tr>
<tr>
<td>Administration Server, Real-Time and Historical Data Server, and Detail Data Server (AW-HDS-DDS)</td>
<td></td>
</tr>
<tr>
<td>Administration Server and Real-Time and Historical Data Server (AW-HDS)</td>
<td><strong>Large Deployment Size</strong></td>
</tr>
<tr>
<td>Historical and Detail Data Server (HDS-DDS)</td>
<td></td>
</tr>
</tbody>
</table>

c) Click **Next**.

**Step 5**
On the Server Role in a Small to Medium Deployment or Server Role in a Large Deployment page, select one of the following options:
Set Up Unified CCE Central Controller Components

- Administration Server and Real-time Data Server (AW)
- Configuration-Only Administration Server
- Administration Server Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS).

**Step 6** Click Next.

**Step 7** Designate the primary and secondary servers for Side A or Side B.

To designate the Side A servers, on the Administration & Data Servers Connectivity page for Side A:

- **a)** Click the radio button for Primary Administration & Data Server.
- **b)** In the Secondary Administration & Data Server field, enter the hostname for the Side B server.
- **c)** In the Primary/Secondary Pair (Site) Name field, enter UCCE.
- **d)** Click Next.

To designate the Side B servers, on the Administration & Data Servers Connectivity page for Side B:

**Note** If you select a server role that includes an HDS, the Secondary Administration & Data Server radio button is dimmed because an HDS is only supported on a Primary Administration & Data Server. Continue with Step 8.

- **a)** Click the radio button for Secondary Administration & Data Server.
- **b)** In the Primary Administration & Data Server field, enter the hostname for the Side A server.
- **c)** In the Primary/Secondary Pair (Site) Name field, enter UCCE.
- **d)** Click Next.

**Step 8** On the Database and Options page, configure as follows:

- **a)** In the Create Database(s) on Drive field, choose C.
- **b)** Check Configuration Management Service (CMS) Node.
- **c)** Check Internet Script Editor (ISE) Server.
- **d)** Click Next.

**Step 9** On the Central Controller Connectivity page, configure as follows:

- **a)** For Router Side A, enter the Call Server Side-A Public Interface or, for an external server, enter the IP address of the Unified CCE Call Server A.
- **b)** For Router Side B, enter the Call Server Side-B Public Interface or, for an external server, enter the IP address of the Unified CCE Call Server B.
- **c)** For Logger Side A, enter the Data Server Side-A Public Interface or, for an external server, enter the IP address of the Unified CCE Data Server A.
- **d)** For Logger Side B, enter the Data Server Side-B Public Interface or, for an external server, enter the IP address of the Unified CCE Data Server B.
- **e)** Enter the Central Controller Domain Name.
- **f)** Select Central Controller Side A Preferred or Central Controller Side B Preferred.
- **g)** Click Next.

**Step 10** Review the Summary page, and then click Finish.
Set up Peripheral Gateways

To set up all the following types of Peripheral Gateways (PG), complete the procedures in this section:

- Cisco Unified Communications Manager PG (CUCM PG)
- Voice Response Unit PG (VRU PG)
- Media Routing PG (MR PG)
- Unified CCE Gateway PG (UCCEnterprise Gateway PG)

Configure Peripheral Gateways

Follow this procedure to complete the first portion of PG configuration. After this procedure, you add a peripheral to the PG; you cannot save the configuration unless there is at least one peripheral in the configuration.

Not all fields apply to all PG types.

Procedure

**Step 1**
Open the PG Explorer tool.

**Step 2**
Click Retrieve, then click Add PG.

**Step 3**
Complete the Logical Controller section as follows:

a) **Logical Controller ID**—Leave blank. This value is generated automatically when the record is saved.

b) **Physical Controller ID**—Leave blank. This value is generated automatically when the record is saved.

c) **Name**—Enter a unique enterprise name for the PG.

d) **Client Type**—Select as follows from the drop-down list:

   - For a CUCM PG: CUCM
   - For a VRU PG: VRU
   - For an MR PG: MR
   - For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

e) **Configuration Parameters**—Leave blank.

f) **Description**—Enter any other information about the PG. Configuration Manager copies this value to the description fields of the logical interface controller, physical interface controller, peripheral, and (if applicable) the routing client records.

g) **Physical Controller Description**—Enter a description for the physical controller.

h) **Primary CTI Address**—Enter the address for the primary CTI server. Make this entry in the form of <IP address or server name where the CTI server is installed>: <Client Connection Port Number>.

i) **Secondary CTI Address**—Enter an address for a secondary CTI server (for duplexed systems).

j) **Reporting Interval**—Select the 15 or 30 Minute reporting interval option (default is 30 Minute). Unified CCE software stores historical information in either half-hour or 15-minute summaries (but not both),
based on the reporting interval value that you set. The Router sends these records to the Logger, which in turn writes them to the Central Database.

**Step 4** Do not exit the PG Explorer tool. You add a peripheral to the PG and save the configuration in the next procedure.

---

### Add Peripherals to Peripheral Gateways

Fields can vary according to PG type.

**Procedure**

**Step 1** With the PG record open in the PG Explorer tool, highlight the PG icon in the tree hierarchy in the lower-left corner of the window.

**Step 2** On the Peripheral tab, enter the following:

a) **Name**—Enter a unique enterprise name for this peripheral.

b) **Peripheral Name**—Enter the name of the peripheral as it is known at the site. Unlike the Enterprise Name field, the value of this field does not have to be unique. For example, at each site you can label the peripherals Switch1, Switch2, and so forth.

c) **Client Type**—Select as follows:
   • For a CUCM PG: CUCM
   • For a VRU PG: VRU
   • For an MR PG: MR
   • For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

d) **Location**—Enter the peripheral's location, for example, the name of a city, building, or department.

e) **Abandoned Call Wait Time**—Enter the minimum time (in seconds) an incoming call must be queued before being considered an abandoned call if the caller hangs up.

f) **Configuration Parameters**—As desired, enter a string containing any parameters that must be sent to the device to initialize it. In most cases, you leave this field blank.

g) **Peripheral Service Level Type**—The default type of service level calculation that the peripheral performs for its associated services. Select *Calculated by Call Center*.

h) **Call Control Variable Map**—As desired, enter a string that describes the mappings of the peripheral call control variables to Unified CCE call control variables.

i) **Agent Phone Line Control**—Specify one of the following agent phone line control options:
   • **Single Line**: Enables single-line monitoring and reporting (default).
   • **All Lines**: Enables multiline monitoring and reporting.

j) **NonACD Line Impact**—Specify one of the following nonACD line impact options:
   • **Available Agent Goes Not Ready**: Agent state is set to Not Ready with a system reason code when the agent answers or calls out on a secondary line while in the Available or Not Ready state.
- **Available Agent Stays Available**: Agent state is unchanged when agent is on a call on a secondary line.

k) **Description**—As desired, enter any additional information about the peripheral.

l) **Default Desk Settings**—Select as follows:
   - For a CUCM PG: Select the Agent Desk Settings that you created earlier
   - For a VRU PG: None
   - For an MR PG: None
   - For a UCC Enterprise Gateway PG: None

m) **Enable Post Routing**—Check this check box to enable the Unified Communications Manager peripheral to send route requests to the Router. When you check this check box, the Routing Client tab is enabled.

**Step 3**

On the Advanced tab, enter the following:

a) **Available Holdoff Delay**—Set this field to zero.

b) **Answered Short Calls Threshold**—Maximum duration, in seconds, for a short call. Any calls with a duration below the threshold are considered short. You can choose to exclude short calls from handle times you calculate.

c) **Network VRU**—The type of network VRU. Select as follows:
   - For a CUCM PG: None
   - For a VRU PG: Select the corresponding Network VRU that you created earlier.
   - For an MR PG: Select the Type 2 Network VRU that you created earlier.
   - For a UCC Enterprise Gateway PG: None

d) **Agent Auto-Configuration**—Not supported for Unified CCE. Leave this option disabled.

e) **Internal IPTA Only**—Be sure that you check this check box for the Unified CCE System PG.

f) **Agent Targeting Mode**—Determines how the Router builds the labels. Select **Rule Preferred**. When this check box is checked, only the local PG can target agents on the PG. The Router uses the skill group IPTA configuration to select agents. When this check box is unchecked, for calls routed between different PGs, the Router picks the agent (which minimizes the benefit of the Unified CCE System PG). Unchecking the check box also requires the creation of more device targets.

**Step 4**

On the Agent Distribution tab, enter the following:

a) **Enable Agent Reporting**—Check to allow Unified CCE reporting on agents.

b) **Agent Event Detail**—Enables label text (as opposed to numeric) Not Ready Reason Code reporting.

c) The Agent Distribution Entries section of this tab contains entries for agent Administration & Data Servers available for distributing agent report data for the selected peripheral. Click **New**, then define the values in the Currently Selected site section of this tab as follows:

   - **Administration & Data Server site name**: The name of the currently selected site in the agent distribution entries list. For MR PGs, do not specify a name for this field.

   - **Agent real time data**: Check to enable the flow of agent real-time data from the peripheral to the Administration & Data Server. Uncheck to disable the flow of agent real-time data.
**Agent historical data:** Check to enable the flow of agent historical data from the peripheral to the Administration & Data Server. Uncheck to disable the flow of agent historical data.

**Step 5** On the Routing Client tab, enter the following:

- **Name**—An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.
- **Timeout threshold**—The maximum time, in milliseconds, the routing client can wait for a response to a routing request.
- **Late threshold**—The threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the Timeout threshold.
- **Timeout limit**—The maximum time, in seconds, for which the routing client waits for a response. If the routing client receives no responses from the Unified CCE system within this limit, it terminates routing operation.
- **Default media routing domain**—Enter Logical ID, Physical ID, and Peripheral ID.
- **Default call type**—Use this call type for any route request that does not match a defined call type mapping. The drop-down list contains all configured call types. The Unified CCE uses the default call type for any routing request from the routing client that does not otherwise map to a call type. If you do not define a default call type for the routing client, the Unified CCE uses a general default call type if you define one through the System Information command.
- **Configuration parameters**—Leave blank.
- **Dial Number/Label map**—Indicates whether only specific labels are valid for each dialed number associated with this routing client (when selected) or whether all labels associated with the routing client are valid for any dialed number (when not selected). Leave unchecked.
- **Client Type**—Select as follows from the drop-down list:
  - For a CUCM PG: CUCM
  - For a VRU PG: VRU
  - For an MR PG: MR
  - For a UCC Enterprise Gateway PG: UCC Enterprise Gateway
- **Description**—More information about the routing client.
- **Network routing client**—A name used to associate routing clients across instances.
- **Network transfer preferred**—If this check box is checked, indicates that network transfer is preferred. When the target of a call is reachable by both a label defined for the requesting routing client and by another label defined for the network routing client that prerouted the call, this option indicates which choice is preferred.

**Step 6** Click **Save**.

**Step 7** Record the Logical Controller ID and Peripheral ID for subsequent use in setting up the PG.

**Configure Peripheral Gateways**

For MR PGs, be aware that you can only set up two PGs per server. Also consider the impact to overall performance. For Outbound Option, configure one peripheral for each Dialer on the MR PG.
Procedure

Step 1
Open the Peripheral Gateway Setup Tool.

Step 2
Select the instance.

Step 3
Click Add in the Instance Components section.

Step 4
Enable the PG on both sides of the Router if you did not enable the PG when you added the Routers:

a) Open the Web Setup Tool for each Router machine and select Routers in the left pane of the page.

b) Check the check box of the Router you want to edit, and click Edit.

c) Proceed through the Edit Router pages until you come to the page where you enable the PG. Add the PG number or range and click Finish.

Step 5
Return to the Peripheral Gateway Setup Tool and complete the following steps in the Peripheral Gateway Properties dialog box.

a) Choose Production Mode. Do not set the Auto Start feature until after the installation is complete.

b) Specify whether the PG is part of a duplexed pair.

c) In the ID field, select from the drop-down list the PG device number as enabled in the Router.

d) If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplexed, select Side A.

e) In the Client Type Selection section of the window, select the client type:

   - For a CUCM PG: CUCM
   - For an MR PG: MR
   - For a VRU PG: VRU
   - For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

Step 6
Click Add.

Step 7
Enter the Logical Controller ID generated when you configured the PG. Click Add and select PIM 1 from the list.

Step 8
Configure the PG properties:

a) To put the PIM into service, check the Enabled option. Enabling the PIM allows it to communicate with the peripheral when the Peripheral Gateway is running.

b) Enter the peripheral name in the Peripheral name field. In most cases, the enterprise name from the associated Peripheral record is the most appropriate name to use. When creating peripheral names, use short descriptive names and keep the length to a minimum.

c) Enter the Peripheral ID that you created when you configured the PG.

d) (MR PG) In Application Hostname (1), enter the hostname or the IP address of the multichannel application server machine. If you are configuring the Outbound Option PIM, enter the IP address or hostname of the BA_IP Dialer.

e) (MR PG) In Application Connection Port (1): for Outbound Option, enter the connection port for the BA_IP Dialer to use. Otherwise, accept the default port number (38001) on the application server machine that the PIM uses to communicate with the application.

f) If two applications interact with the Unified CCE, in Application Hostname (2), enter the hostname or the IP address of the second application server machine. If you are using the hostname, the name must be in the hosts file.
g) If two applications interact with the Unified CCE, in Application Connection Port (2), enter the port number on the second application server machine that the PIM uses.

h) For Heartbeat Interval (seconds), specify how often the PG checks its connection to the call server. Use the default value.

i) For Reconnect Interval (seconds), specify how often the PG should try to reestablish a lost connection to the call server. Use the default value.

j) Click OK.

Step 9

From the Peripheral Gateway Component Properties window, click Next. The Device Management Protocol Properties window appears.

a) Enter the appropriate settings and click Next. The Peripheral Gateway Network Interfaces window appears.

b) Enter the appropriate settings and click Next. The Check Setup Information window appears.

Step 10

Verify the setup information and click Next.

Step 11

When the Setup Complete window appears, click Finish.

---

Install JTAPI Client on Unified Communications Manager PG

After setting up the Unified Communications Manager PG, you must install the Cisco JTAPI Client so that the PG can communicate using JTAPI with the Unified Communications Manager. You install the Cisco JTAPI Client from Unified Communications Manager Administration.

**Procedure**

**Step 1**
Open a browser window on the PG machine.

**Step 2**
Enter the URL for the Unified Communications Manager Administration utility: http://<Unified Communications Manager machine name>/ccmadmin.

**Step 3**
Enter the username and password that you created when installing and configuring the Unified Communications Manager.

**Step 4**
Choose ApplicationPlugins. Click Find.

**Step 5**
Click the link next to Download Cisco JTAPI for Windows. Download the 32 bit version only.

**Step 6**
Choose Save and save the file to a location of your choice.

**Step 7**
Open the installer.

**Step 8**
In the Security Warning box, click Yes to install.

**Step 9**
Choose Next or Continue through the remaining Setup screens. Accept the default installation path.

**Step 10**
Click Finish.

**Step 11**
Reboot the machine.

---

Set up CTI Server

Use the PG Setup tool to set up a CTI Server.


**Add CTI Server Component**

**Procedure**

**Step 1** In the PG Setup dialog box, in the left column under ICM Instances, select an instance.

**Step 2** Click **Add** in the Instance Components section.
The ICM Component Selection dialog box opens.

**Step 3** Click **CTI Server**.
The CTI Server Properties dialog box opens.

**Set CTI Server Properties**

**Procedure**

**Step 1** In the CTI Server Properties dialog box, check **Production mode** and **Auto start at system startup** unless your Unified CCE support provider tells you otherwise. These settings set the CTI Server Service startup type to Automatic, so the CTI Server starts automatically when the machine starts up.

**Step 2** Check the **Duplexed CTI Server** option if you are configuring redundant CTI Server machines.

**Step 3** In the CG Node Properties section, the numeric portion of the CG node **ID** must match the PG node ID (for example, CG 1 and PG 1).

**Step 4** The **ICM system ID** is the Device Management Protocol (DMP) number of the PG associated with the CTI Gateway. Generally this number is the number associated with the CG ID in step 3.

**Step 5** If the CTI Server you add is duplexed, specify which **Side** you are setting up: Side A or Side B. If the CTI Server is simplex, choose Side A.

**Step 6** Click **Next**.
The CTI Server Component Properties dialog box opens.

**Set CTI Server Component Properties**

**Procedure**

**Step 1** In the CTI Server Component Properties dialog box, setup automatically generates a **Client Connection Port Number**. You can use this value or change to a standard port number. Clients use this port number to connect to the CTI Server.

If you have multiple nodes running on a single machine, each must use a different port number.
Step 2  If you require that an agent is logged in to the client before the client receives events from the CTI Server, check the Agent Login Required for Client Events box. When you check this box, clients are prevented from accessing data for other agents.
Step 3  Click Next.
The CTI Server Network Interface Properties dialog box opens.

Set CTI Server Network Interface Properties

Procedure

Step 1  In the CTI Server Network Interface Properties dialog box, in the PG public interfaces section, enter the public network addresses for the PGs associated with the CTI Server.
Step 2  In the CG private interfaces section, enter the private network addresses of the CTI Server.
Step 3  In the CG visible interfaces section, enter the visible network addresses of the CTI Server.
Step 4  Click Next.
The Check Setup Information window opens.

Complete CTI Server Setup

Procedure

Step 1  In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the Back button.
Step 2  When the settings are correct, click Next.
Step 3  The final screen displays and asks whether you want to start the Node Manager now.
Step 4  Click Finish to exit setup (and optionally start the Node Manager).
If you choose to start it, the Node Manager automatically starts the other Unified CCE processes on the CTI Server.

Install Unified CCE Administration Client

Install Administration Client

Do not install the Administration Client on a system that already has other Unified CCE software installed; the Administration Client must reside on a standalone machine.
Procedure

**Step 1**  Navigate to the `AdminClientInstaller` directory and double-click the `setup.exe` program. The Administration Client Installer program proceeds through a series of screens on which you specify information.

**Step 2**  When the installation is complete, reboot the server.

---

**Set up Administration Client**

You cannot run the Administration Client Setup tool remotely through a browser. Run the tool on the local machine.

**Before You Begin**

Any user who is a local administrator on the machine and a domain user can log in. However, to view the lists and to perform tasks with the Administration Client Setup tool, you must have the following permissions:

- Administrator on the local machine
- Either a domain administrator or a member of at least one Setup security group in the machine domain.

If you cannot add an Administration Client instance on a Windows 7 system, check whether Cisco Security Agent is installed. Cisco Security Agent is deprecated, uninstall it if you find it on a system.

Procedure

**Step 1**  Open the Administration Client Setup tool.
**Step 2**  Sign in as a domain user with local Administrator rights.
**Step 3**  Click **Instance Management**, and then click **Add**.
**Step 4**  On the Add Instance page, from the drop-down list, choose the customer facility and instance.
**Step 5**  Enter an instance number. The same instance name can occur more than once in a domain, so the instance number provides the uniqueness. The instance number must be between 0 and 24. The instance number must match for the same instance across your entire deployment. For an Enterprise (single instance) deployment, select 0 unless there is a reason to choose another value.
Install Unified CCE Language Pack

Run the Language Pack Installer to install any of the following non-English localized files for the Script Editor:

- French (France)
- French (Canada)
- Japanese
- Chinese (Simplified)

Before You Begin


Note

If the Unified CCE language pack is applied on a Chinese Windows machine, set the screen resolution to 1600 x 1200.

Procedure

Step 1 Go to the Download Software page and log in using your Cisco.com credentials.
Step 2 Download the Language Pack installer.
Step 3 Open the installer and follow the instructions.
Update the Java Runtime Environment (Optional)

The main Unified CCE Installer installs the Java Runtime Environment (JRE) to a default location (for example, C:\Program Files (x86)\Java\jre1.7.0_51) and creates a JAVA_HOME environment variable set to that location. In most circumstances, you do not need to modify or configure the JRE after the Unified CCE installation. For information on the version installed, see the Java requirements in the Unified CCE Solution Compatibility Matrix at http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE.

If you have requirements for a different version of the JRE, you can update the JRE installed by the Unified CCE installation.

To update the Unified CCE JRE to a later version:

1. Review the Java requirements in the Unified CCE Solution Compatibility Matrix to confirm that Unified CCE supports the JRE version you want to install.
2. Follow the Oracle JRE installer procedure to install the JRE to the VM on which your Unified CCE components are installed.
3. Set the JAVA_HOME environment variable to the location of the new JRE.
4. Restart the virtual machine.

When you have completed the update to the new JRE version, uninstall the old JRE.

Note

The ICM-CCE-CCHInstaller installs JRE 1.7, build 51 during the installation. If an older version of JRE is currently installed on the deployment machine, it will not be uninstalled by the installer.

Silent installation

In certain situations, such as when a system administrator wants to install or upgrade software automatically on multiple systems simultaneously, a silent installation is preferable to running an installation wizard. You can run a silent installation when performing a fresh install or an upgrade.

Silent installation prerequisites

Before running a silent installation, complete the following tasks:

- Stop all applications that are running on the system.
- By default, silent installation assumes the following parameter: Install on Drive C. To override this default, edit the ICMCCSilentSetup.ini file in the ICM-CCE-CCH Installer directory.
- Mount the ISO image to the target machine, and make the following edits on the target machine:
  - If you are performing a Technology Refresh upgrade, change the szInstallType from 0 to 1. The default value of 0 is for a Fresh Install.
  - If you are performing a Technology Refresh upgrade, provide a path for the szExportedRegistryPath parameter.
To change the drive on which you are installing the application, change the **szDrive** parameter.
Replace C with the drive where you want to install.

If you do not want to apply SQL Security Hardening, change the line that reads **szSQLSecurity=1**
to **szSQLSecurity=0**.

**Note**
You can apply SQL Security Hardening during the installation, or you can use the Security Wizard to apply it after the install.

---

**Perform a silent installation**

**Procedure**

**Step 1**
Mount the Installation ISO image to the target machine.

**Step 2**
From a command prompt window, navigate to the ICM-CCE-CCH Installer directory.

**Step 3**
Enter the command `setup.exe /s`.

The installation application runs. The drive prompt reappears in the command prompt window when the installation is complete.

**Note**
If the installation is not successful, no error message appears in the command prompt window. You must check the installation log file `<SystemDrive>:\temp\ICMInstall.log` to determine the reason why the installation failed.

---

**Cisco Finesse Server Installation**

Cisco Finesse server is installed on a virtual machine (VM). The installation runs from an ISO image and uses an OVA template.

**Note**
For a new installation of Finesse, you can install directly from the latest ES. You do not need to install the base version and then apply the latest ES.

**Note**
Configure a DataStore ISO file on the virtual CD/DVD drive of the target VM to install Finesse.

The installation takes about an hour. For most of that time, it can run unattended. 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.
Installation Task Flow

The following table provides an overview of the tasks you perform to install Cisco Finesse. Tasks must be performed in the order they are listed.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Install Finesse on the primary node.</td>
<td>See Install Finesse on Primary Node, on page 60.</td>
</tr>
<tr>
<td><strong>2</strong> Configure the CTI server settings.</td>
<td>See Configure Contact Center Enterprise CTI Server Settings, on page 62.</td>
</tr>
<tr>
<td><strong>3</strong> Configure the database settings.</td>
<td>See Configure Contact Center Enterprise Administration &amp; Data Server Settings, on page 63.</td>
</tr>
<tr>
<td><strong>4</strong> Configure the cluster settings for the secondary node.</td>
<td>See Configure Cluster Settings, on page 64.</td>
</tr>
<tr>
<td><strong>5</strong> Restart Cisco Finesse Tomcat on the primary node.</td>
<td>See Restart Cisco Finesse Tomcat, on page 65.</td>
</tr>
<tr>
<td><strong>6</strong> Install Finesse on the secondary node.</td>
<td>See Install Finesse on Secondary Node, on page 65.</td>
</tr>
<tr>
<td><strong>7</strong> Ensure replication is functioning between the two nodes.</td>
<td>See Check Replication Status, on page 68.</td>
</tr>
<tr>
<td><strong>8</strong> Install language packs (optional).</td>
<td>See Install Language Pack.</td>
</tr>
</tbody>
</table>
Install Finesse on Primary Node

Procedure

Step 1 Follow the instructions in the OVA README.txt file to import and deploy the OVA, to edit VM settings, and to power on the VM and edit the BIOS settings in the console.

Note Do not use Thin Provisioning or a VM snapshot when creating a VM to host Cisco Finesse. The use of Thin Provisioning or snapshots can negatively impact the performance of Cisco Finesse operation. Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

Step 2 Select Yes on the DVD Found screen to begin the verification of the media integrity and a brief hardware check.
If the media check passes, select OK to open the Product Deployment Selection screen. Continue to Step 3.
If the media check fails, the installation terminates.

Step 3 The Product Deployment Selection screen states that the Cisco Finesse product suite will be installed. This screen has only one choice: OK.
Select OK to open the Proceed with Install screen.

Step 4 The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE. Select Yes on the Proceed with Install screen to open the Platform Installation Wizard screen.

Step 5 On the Platform Installation Wizard screen, select Proceed to open the Basic Install screen.

Step 6 Select Continue on the Basic Install screen to open the Basic Install wizard.
The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.
The first Basic Install wizard screen is Timezone Configuration.

Step 7 On the Timezone Configuration screen:
   a) Use the up and down arrows to locate the local time zone that most closely matches your server location.
      You can also type the initial character of the time zone to move to that item in the list. The Timezone field is based on country and city and is mandatory. Setting it incorrectly can affect system operation.
   b) Select OK to open the Auto Negotiation Configuration screen.

Step 8 On the Auto Negotiation Configuration screen, select Continue to use automatic negotiation for the settings of the Ethernet network interface card (NIC).
The MTU Configuration screen appears.

Step 9 In the MTU Configuration screen, select No to keep the default setting for Maximum Transmission Units (1500).
Note Finesse supports the default setting of 1500 for MTU only. No other value is supported.
Your selection of No opens the Static Network Configuration screen.

Step 10 On the Static Network Configuration screen, enter static network configuration values as follows, referring to the Configuration Worksheet if necessary:
   a) Enter the Host Name.
   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 11**  
On the DNS Client Configuration screen, select **Yes** to specify the DNS client information.

*Important*  
DNS client configuration is **mandatory** for Cisco Finesse. Select Yes on this screen. If you select No, after the installation is complete, agents **cannot** sign in to the desktop and you have to reinstall Finesse.

**Step 12**  
Specify your DNS client information as follows, referring to the Configuration Worksheet 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 13**  
On the Administrator Login Configuration screen:

a) Enter the credentials for the administrator.
b) Select **OK** to open the Certificate Information screen.

**Step 14**  
On the Certificate Information screen:

a) Enter the following data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country.
b) Select **OK** to open the First Node Configuration screen.

**Step 15**  
On the First Node Configuration screen, select **Yes** to indicate that you are configuring the first node. Your selection of Yes opens the Network Time Protocol Client Configuration screen.

**Step 16**  
On the Network Time Protocol Client Configuration screen, enter the IP address, NTP server name, or NTP Server Pool name for at least one external NTP server.

**Step 17**  
After you complete the NTP configuration, select **OK**. This action opens the Security Configuration screen.

**Step 18**  
On the Security Configuration screen, enter the Database Access Security password, and then select **OK**.

**Step 19**  
On the Application User Configuration screen, enter the credentials for the application user.
Select **OK** to open the Platform Configuration Confirmation screen. This screen states that the platform configuration is complete.

**Step 20**  
On the Platform Configuration Confirmation screen, select **OK**.

The installation begins.

The installation can take up to an hour to complete and can run unattended for most of that time.

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

- Formatting progress bars
- Copying File progress bar
- Package Installation progress bars
- Post Install progress bar
- Populate RPM Archive progress bar
- Application Installation progress bars (multiple Component Install screens, security checks)
- An informational screen saying the system will reboot momentarily to continue the installation
If you see the following virtual machine question, select Yes, and then click OK:

**Figure 1: Virtual Machine Message**

---

- **A system reboot**
  
  Messages stream down your monitor during the reboot. Some of them 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 appears during the Configure and Setup Network process, click **Review**, and then click **OK** at the Errors screen. Follow the prompts to reenter the information that caused the failure. The installation continues when the connection information is complete.

- **Security configuration**

A message appears that states the installation of Cisco Finesse has completed successfully.

```
The installation of Cisco Finesse has completed successfully.
Cisco Finesse <version number>
<hostname> login: _
```

**What to Do Next**

Sign in to the Finesse administration console on the primary Finesseserver (http://FQDN of Finesse server/cfadmin) to configure CTI server, Administration & Database server, and cluster settings.

After you configure these settings, install Finesse on the secondary node.

**Configure Contact Center Enterprise CTI Server Settings**

Access the administration console on the primary Finesseserver to configure the A Side and B Side CTI servers.
After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to access the Finesse administration console.

Note
If you are using HTTPS, the first time you access the administration console, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

Procedure

Step 1
Sign in to the administration console on the primary Finesse server:
http://FQDN of Finessse server/cfadmin

Step 2
Sign in with the Application User credentials defined during installation.

Step 3
In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Side Host/IP Address</td>
<td>Enter the hostname or IP address of the A Side CTI server.</td>
</tr>
<tr>
<td></td>
<td>This value is typically the IP address of the Peripheral Gateway (PG).</td>
</tr>
<tr>
<td></td>
<td>The CTI server runs on the PG.</td>
</tr>
<tr>
<td>A Side Port</td>
<td>Enter the port number of the A Side CTI server.</td>
</tr>
<tr>
<td></td>
<td>The value of this field must match the port configured during the setup of</td>
</tr>
<tr>
<td></td>
<td>the A Side CTI server.</td>
</tr>
<tr>
<td>Peripheral ID</td>
<td>Enter the ID of the Agent PG Routing Client (PIM).</td>
</tr>
<tr>
<td></td>
<td>The Agent PG Peripheral ID should be configured to the same value for the</td>
</tr>
<tr>
<td></td>
<td>A Side and B Side CTI servers.</td>
</tr>
<tr>
<td>B Side Host/IP Address</td>
<td>Enter the hostname or IP address of the B Side CTI server.</td>
</tr>
<tr>
<td>B Side Port</td>
<td>Enter the port of the B Side CTI server.</td>
</tr>
<tr>
<td></td>
<td>The value of this field must match the port configured during the setup of</td>
</tr>
<tr>
<td></td>
<td>the B Side CTI server.</td>
</tr>
</tbody>
</table>

Step 4
Click Save.

Configure Contact Center Enterprise Administration & Data Server Settings

Configure the Contact Center Enterprise Administration & Data Server settings to enable authentication for Finesse agents and supervisors.
### Configure Cluster Settings

Configure the cluster settings for the secondary Finesse node. The secondary Finesse node handles agent requests if the primary server goes down.

#### Procedure

**Step 1** If you are not already signed in, sign in to the administration console with the Application User credentials.

**Step 2** In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.

**Step 3** Click Save.
Restart Cisco Finesse Tomcat

After you make changes to the Contact Center Enterprise CTI Server, Contact Center Enterprise Administration & Data Server, or cluster settings, restart Cisco Finesse Tomcat for the changes to take effect.

Procedure

**Step 1**
Access the CLI and run the following command:
```
utilsservicerestartCiscoFinesseTomcat
```

**Step 2**
You can enter the command `utilsservice list` to monitor the Cisco Finesse Tomcat Service. After Cisco Finesse Tomcat changes to STARTED, agents who have passwords can sign in to the desktop.

Install Finesse on Secondary Node

Install the same version of Finesse on both the primary and secondary Finesse nodes.

**Note**
Configure a Datastore ISO file on the virtual CD/DVD drive of the target VM to install Finesse.

**Note**
Finesse administration tasks can only be performed on the primary Finesse server. After you install the secondary server, sign in to the administration console on the primary server to perform administration tasks (such as configuring reason codes or call variable layout).

**Before You Begin**
- Install Finesse on the primary server.
- Use the Finesse administration console on the primary Finesse server to configure CTI server, Administration & Database server, and cluster settings.
- Ensure that the DNS server has forward and reverse DNS set up for both the primary and secondary node.

**Procedure**

**Step 1**
Follow the instructions in the OVA README.txt file to import and deploy the OVA, to edit VM settings, and to power on the VM and edit the BIOS settings in the Console. Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

**Step 2**
Select Yes on the DVD Found screen to begin the verification of the media integrity and a brief hardware check.
If the media check passes, select OK to open the Product Deployment Selection screen. Continue to Step 3.
If the media check fails, the installation terminates.

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

**Step 4** The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE. Select **Yes** on the Proceed with Install screen to open the Platform Installation Wizard screen.

**Step 5** On the Platform Installation Wizard screen, select **Proceed** to open the Basic Install screen.

**Step 6** Select **Continue** on the Basic Install screen to open the Basic Install wizard. The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.

The first Basic Install wizard screen is Timezone Configuration.

**Step 7** In the Timezone Configuration screen:
   a) Use the up and down arrows to locate the local time zone that most closely matches your server location. You can also type the initial character of the time zone to move to that item in the list. The Timezone field is based on country and city and is mandatory. Setting it incorrectly can affect system operation.
   b) Select **OK** to open the Auto Negotiation Configuration screen.

**Step 8** On the Auto Negotiation Configuration screen, select **Continue** to use automatic negotiation for the settings of the Ethernet network interface card (NIC). The MTU Configuration screen appears.

**Step 9** On the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units (1500).

*Note* Finesse supports the default setting of 1500 for MTU only. No other value is supported.

Your selection of No opens the Static Network Configuration screen.

**Step 10** On the Static Network Configuration screen, enter static network configuration values as follows, referring to the Configuration Worksheet if necessary:
   a) Enter the **Host Name**.
   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 11** On the **DNS Client Configuration** screen, select **Yes** to specify the DNS client information.

**IMPORTANT:** DNS client configuration is mandatory for Cisco Finesse. Select Yes on this screen. If you select No, after the installation is complete, agents cannot sign in to the desktop and you have to reinstall Finesse.

**Step 12** Specify your DNS client information as follows, referring to the Configuration Worksheet 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 13** On the Administrator Login Configuration screen:
   a) Enter the credentials for the administrator.
b) Select **OK** to open the Certificate Information screen.

**Step 14** On the Certificate Information screen:

- a) Enter the following data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country.
- b) Select **OK** to open the First Node Configuration screen.

**Step 15** On the First Node Configuration screen, select **No** to indicate that you are configuring the second node. A warning message appears that indicates you must first configure the server on the first node before you can proceed. If you already configured the first node, select **OK**.

**Step 16** On the Network Connectivity Test Configuration screen, select **No** to proceed with the installation after connectivity is verified.

**Step 17** On the First Node Configuration screen, specify the information about the first node as follows:

- a) Enter the **HostName** of the primary Finesse server.
- b) Enter the **IPAddress** of the primary Finesse server.
- c) Enter the **SecurityPassword** of the primary Finesse server.
- d) Confirm the **SecurityPassword**.

**Step 18** Select **OK** to open the Platform Configuration Confirmation screen.

**Step 19** On the Platform Configuration Confirmation screen, select **OK**. The installation begins.

The installation can take up to an hour to complete and can run unattended for most of that time.

A message appears that states the installation of Cisco Finesse has completed successfully.

The installation of Cisco Finesse has completed successfully.

_Cisco Finesse <version number>
<hostname> login: _

---

**What to Do Next**

Check the replication status. If all nodes in the cluster show a replication status of **2**, replication is functioning correctly.

---

**Note**

It can take 10–20 minutes to establish replication fully between the two nodes.

---

**Upgrade VMware Tools**

To ensure that your version of the VMware Tools is current, refresh the installed version of VMware Tools from the local VMware host on both Finesse nodes.
Procedure

Step 1  Log in to the primary Finesse node.
Step 2  Run the command to update the VMware Tools: `utils vmtools refresh`
Step 3  Log in to the secondary Live Data Finesse node.
Step 4  Run the command to update the VMware Tools: `utils vmtools refresh`

Check Replication Status

Procedure

Step 1  Access the CLI on the primary Finesse server.
Step 2  Sign in with the Administrator User credentials defined during installation.
Step 3  Run the following command:

```
utils dbreplication runtimestate
```

This command returns the replication status on both the primary and secondary Finesse servers.
Initial Configuration

- Initial Configuration Overview, page 69
- Initial Configuration Task Flow, page 69
- Initial Configuration Tasks, page 70

Initial Configuration Overview

This initial configuration brings the contact center to the point where a complete call flow is possible. The configured system will process information about incoming calls, perform call routing, and enable call handling.

Related Topics

- Initial Configuration Task Flow, on page 69

Initial Configuration Task Flow

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Cisco Unified Contact Center Enterprise</td>
<td>Configure Cisco Unified Contact Center Enterprise, on page 70</td>
</tr>
<tr>
<td>Configure Cisco Unified Intelligence Center</td>
<td>Configure Cisco Unified Intelligence Center, on page 112</td>
</tr>
<tr>
<td>Configure Cisco Unified Customer Voice Portal</td>
<td>Configure Cisco Unified Customer Voice Portal, on page 118</td>
</tr>
<tr>
<td>Configure Cisco Unified Communications Manager</td>
<td>Configure Cisco Unified Communications Manager, on page 130</td>
</tr>
<tr>
<td>Configure Cisco Finesse</td>
<td>Configure Cisco Finesse, on page 147</td>
</tr>
</tbody>
</table>
Initial Configuration Tasks

Configure Cisco Unified Contact Center Enterprise

You can configure individual records, or you can use the Bulk Configuration tool to configure multiple records at one time. Bulk configuration is available for the following:

- Agents
- Call types
- Dialed number plans
- Dialed numbers
- Labels
- Network trunk groups
- Network VRU scripts
- Peripheral targets
- Persons
- Regions
- Region prefixes
- Routes
- Trunks
- Trunk groups
- Scheduled targets
- Services
- Skill groups
- VRU port maps

Related Topics

Perform Bulk Configuration, on page 106

Access Configuration Manager tool

You perform all Unified CCE configuration tasks using the Configuration Manager tool, which is installed with the Unified CCE software.

1. From your desktop, double-click the Unified CCE Tools icon, and then select Administration Tools.
2. Click the Configuration Manager icon.
Configure Media Routing Domain

You must establish Media Routing Domains (MRD) for each multi-media class that your Unified CCE System supports. Valid media classes are: multi-session chat, single-session chat, blended collaboration, email, and voice. An MRD for the voice media class is installed by default with your Unified CCE software. You do not need to create an MRD for the voice media class.

Procedure

Step 1  Start the Configuration Manager and select Tools > List Tools > Media Routing Domain List.

Step 2  Click Retrieve and then click Add.

The Attributes tab appears.

Step 3  On the Attributes tab, provide values for the following fields:

Name. Enter the enterprise name of the MRD.

Media Class. Use the drop-down list to select the media class for the integrated application.

Max Time in queue. The default maximum queue time for calls in queue is one hour. To override this default, modify the value of the Max Time In queue field.

The MR domain ID is automatically generated when you save the MRD.

Step 4  After completing the required fields, click Save.

Repeat this procedure to add an MRD for each media class that your system supports.

Configure trunk groups

For the Unified CCE, the Network Trunk Group is the placeholder in the Unified CCE database for the trunk group; it performs no other function.

For deployments that:

- Use the Unified CCE System PG, you must create one Network Trunk Group for each Unified CCE System PG peripheral.

- Do not use the Unified CCE System PG, you must create two Network Trunk Groups—one for the Unified Communications Manager and one for the Unified CVP or Unified IP IVR. If you are deploying the Unified CVP, create one Network Trunk Group per CVP Server.

A Unified CCE Trunk Group is a collection of trunks associated with a single peripheral and usually used for a common purpose. For the Unified CCE, the trunk groups for VRU peripherals are used primarily as a placeholder in the Unified CCE database.

Create a trunk group for each Unified Communications Manager peripheral and a trunk group for each Unified IP IVR application. If you are deploying Unified CVP, you must create two trunk groups for each Unified CVP Server that match the Group Numbers configured in Unified CVP Application Administration. For Unified IP IVR, the trunk group peripheral number in the Unified CCE must match the CTI Port Group ID on Unified IP IVR.

To configure a Network Trunk Group (and the trunk group under it):
**Procedure**

**Step 1** From the Configuration Manager, choose **Configure ICM > Peripherals > Trunk Group > Network Trunk Group Explorer**. The ICM Network Trunk Group Explorer dialog box opens.

**Step 2** Click **Retrieve**.

**Step 3** Click **Add Network Trunk Group**. The Network Trunk Group tab opens.

**Step 4** Add a unique name for the Network Trunk Group and an appropriate description.

**Step 5** Click **Add Trunk Group** to add a trunk group.

**Step 6** Complete these fields:
- **Peripheral**. Select the peripheral to which the trunk group is associated.
- **Peripheral Number**. Enter the number of the trunk group as understood by the peripheral. This number must be unique among all trunk groups associated with the peripheral. For Unified IP IVR, this number must:
  1. Match a CTI Port Group ID configured on the Unified IP IVR.
  2. Be an odd number.
  3. Be unique for all Unified IP IVRs handled by an Unified CCE System PG.

  For example, if a Unified CCE System PG handles four Unified IP IVRs and each Unified IP IVR peripheral has one CTI Port Group, then the CTI Port Group ID for the first Unified IP IVR should be 1, the port group ID for the second Unified IP IVR should be 3, and so on. For the Unified CVP, this number must match a CVP Server Group Number configured on the CVP Server.

- **Peripheral Name**. Enter the name of the trunk group as understood by the peripheral. This name must be unique among all trunk groups associated with the peripheral.

- **Name**. Enter the enterprise name of the trunk group. The Unified CCE forms a default for this name using the entries from the Peripheral and Peripheral Name fields.

- **Extension**. Leave this field blank.

- **Trunk Count**. Select **Use Trunk Data**. When you specify **Use Trunk Data**, the system software determines the trunk count dynamically by counting the associated records in the Trunk table.

- **Configuration Parameters**. Leave this field blank.

- **Description**. Enter an optional description.

**Step 7** To add trunks to the trunk group, click **Add Trunk**.

**Step 8** Add trunks as desired.

**Step 9** Click **Save** and then click **Close**.

**Step 10** Repeat these steps to create all necessary trunk groups.

---

**Configure Network VRU Bank**

The **Network VRU Bank** allows load balancing across multiple VRUs to occur and eliminates the need for complex translation-route configuration.

Configure a Network VRU Bank, only if your deployment uses the Unified CCE System PG.
Before You Begin

Do this after you configure the following:

- Network VRU
- Network Trunk Group
- All other trunk groups

Procedure

Step 1 From the Configuration Manager, choose Explorer Tools > Network VRU Explorer. The Network VRU Explorer dialog box opens.

Step 2 Click Retrieve and select your Network VRU.

Step 3 Select the Network VRU Bank tab and click Add. The Select Trunk Group dialog box opens, displaying the all trunk groups configured on all Unified CCE System PG peripherals.

Step 4 Select the trunk group associated with the translation routing group on your Unified IP IVR. Make the appropriate trunk group selection for each Unified IP IVR in your deployment.

Step 5 Click OK.

Step 6 Click Add Label to add a label for the Network VRU Bank. The label must be the CTI Route Point trigger for the Translation-Routing application on the Unified IP IVR. By default, in the Label tab, the first field shows the selected Network VRU, *not* the Network VRU Bank:

a) Click the drop-down list box to show the available Network VRU banks.

b) Select a Network VRU bank in the drop-down list.

c) Then configure the label for the Network VRU bank.

d) Repeat the steps to configure labels for all of the Network VRU Banks.

If Network VRU Bank labels are available, the Router uses them when it balances the load between the Unified IP IVRs. If the Router cannot find an eligible Network VRU Bank labels, it uses the Network VRU label.

Configure services

A *service* refers to a type of processing that a caller requires. For example, separate services might be defined for Sales, Support, or Accounts Payable. Services are often associated with a peripheral, and are sometimes referred to as peripheral services. An agent is assigned one or more skills that in turn is associated with services. Routing to a Unified CCE service effectively targets an agent assigned to a Unified CCE skill group associated with the Unified CCE service.

Services on the Unified CCE correspond to CTI Route Points on Unified Communications Manager.
On Unified CCE systems that interface with Unified CVP systems, you must configure two services with Peripheral Numbers of 1 and 2. However, outside of these services the preferred method of defining Unified CCE routable tasks is by defining call types.

For the two Unified CVP services, you do not need to configure Service Members, Routes, Peripheral Targets, or Labels.

**Procedure**

**Step 1** From the Configuration Manager menu, choose **Tools > Explorer Tools > Service Explorer**. The Service Explorer dialog box opens.

**Step 2** Select the peripheral for which you want to create a service and click **Retrieve**.

**Step 3** Click **Add Service**.

The Service Configuration window opens.

**Step 4** On the Service tab, enter the following:

- **Media Routing Domain**.
- **Peripheral Number.** Enter the number for the service on the peripheral. This field must be unique for all services for the peripheral, but not necessarily across all peripherals. If you are deploying the Unified CVP, enter 1 for the first service and 2 for the second service.
- **Peripheral Name.** Enter a name that describes the service.
- **Enterprise Name.** Enter an enterprise name for the service. This name must be unique among all the services in the enterprise. If you do not enter a value, this name is autogenerated.
- **Config Param.** Not used for the Unified CCE.
- **Description.** Enter any additional information about the service.
- **Service Level Type.** Indicates how the Unified CCE calculates the service level for the service. You can choose to omit abandoned calls from the calculation, treat them as having exceeded the threshold (negative impact on service level), or treat them as answered calls (positive impact on service level). You can also choose to use the default specified for the peripheral.
- **Service Level Threshold.** Enter the time in seconds, for the service level. The Unified CCE tracks the percentage of calls answered within this threshold. If this field is negative, the value of the default for the peripheral is used.

**Step 5** On the Advanced tab, enter the following:

- **Peripheral Service Level.** Indicates the type of service level calculation that the peripheral performs for this service. This setting has no effect because the PG does not report a peripheral service level.
- **Schedule name.** Identifies an imported schedule associated with the service.

- **Extension.** If you are deploying Outbound Option, enter the extension to associate with this service. This corresponds to a CTI Route Point defined in Unified Communications Manager and is associated with the PG User.

**Step 6** On the Service Members tab, select skill groups to associate with this service.

**Step 7** Click **Apply**.

**Step 8** Repeat this procedure to add any other services.
Configure dialed numbers

The dialed number (DN) is the number that the caller dials to start the call and identifies the Unified CCE routing script to run. Set dialed numbers for ring no answer, dialed number plan entries, and for Supervisor/emergency calls.

For Unified Communications Manager to generate a route request to the Unified CCE, the cluster associates the DN with a CTI Route Point for the Unified CCE JTAPI User. Configure the DN in the Unified CCE. After the Unified CCE receives the route request with the DN, that DN is mapped to a Unified CCE Call type, which is then mapped to a Unified CCE routing script.

Note
You cannot use the DN for a CTI Route Point on a different CTI Route Point in another partition. Ensure that DNs are unique across all CTI Route Points on all partitions.

Unified CCE generates a unique value for the Label Name list after you configure a dialed number.

Procedure

Step 1 From the Configuration Manager, choose Tools > List Tools > Dialed Number/Script Selector List. The Dialed Number/Script Selector List dialog box opens.

Step 2 Click Retrieve and then click Add. The Attributes tab displays.

Step 3 In the Attributes tab, enter values in the following fields:
- **Routing client**: Choose the enterprise name of the routing client associated with this dialed number. After you select a routing client and save to the database, this field becomes read only.
- **Media Routing Domain**: The media routing domain associated with the selected dialed number or script selector.
- **Dialed number string**: Enter the string value that the routing client passes to the Unified CCE for this dialed number (for example: 8005551212).
- **Name**: Enter the enterprise name for the dialed number. This name must be unique among all dialed numbers in the system. If you do not enter a value, the name is autogenerate.
- **Customer**: Use the drop-down list to select the customer (Unified CCE instance) associated with the dialed number.
- **Default label**: Choose the name of the default label for this dialed number. The label must have been previously defined for it to be in the selection list. Use the Label List tool in the Configuration Manager to define labels. If the Unified CCE fails to determine a target for the call within the routing client's time-out threshold, then the default label for the dialed number is used.
- **Description**: Enter a description for the dialed number.
- **Permit application routing**: If you intend to route calls from a parent system to this dialed number, check this dialog box.
Note If you build your software script to capture ECC variables and you want those variables passed to Cisco Agent Desktop agents after they queue to a VRU, then check this check box. This setting enables the data to be sent when a call is queued. Apply the setting for all the dialed numbers to which calls queue.

Reserved by IVR. For VRU dialed numbers, check this box. This setting prevents the CallManager PIM from trying to exert control on the calls arriving on these Route Points.

Step 4 On the DN Mapping tab, as desired, click Add to specify a call type and other dialing information to associate with this dialed number.

Step 5 Click Save to enter the dialed number information.

Step 6 Repeat this procedure for any additional dialed numbers.

Configure call types

A call type is a category of Unified CCE routable task. Each call type has a schedule that determines which routing script or scripts are active for that call type at any time.

There are two classes of call types:

• Voice (phone calls). Voice call types are categorized by the dialed number (DN), caller-entered digits (CED), and calling line ID (CLID). The CED and CLID can be optional, depending on the call.

• Non-voice (email and text chat). Non-voice call types are categorized by the Script Type Selector, Application String 1, and Application String 2. Application String 1 and Application String 2 can be optional, depending on the application.

To facilitate Unified CCE reporting, it is good practice to create separate call types for VRU applications and queuing applications.

Procedure

Step 1 From the Configuration Manager, select Tools > List Tools > Call Type List.

The Call Type List dialog box opens.

Step 2 Click Retrieve and then click Add.

The Attributes tab appears.

Step 3 In the Attributes tab, enter values for the following fields:

Name. Enter an enterprise name for the call type. This name must be unique among call types in the system.

Customer. Choose the customer (Unified CCE Instance) from the drop-down list.

Service level threshold. The service level threshold is the target maximum time that a caller spends in a queue before being connected to an agent. When you set up a peripheral, you specify a default service level threshold for all services associated with that peripheral. If you enter a negative number, the service level threshold from the Peripheral table is used.

This field is prepopulated with the default service level threshold for this peripheral and grayed out. If you wish to override this default, check the Override System Information Default check box to the right of this field and enter a different value.
You can also set the Service Level in the Configuration Manager with the System Information tool. When the service level is defined with the Call Type tool, this setting overrides a setting made with the System Information tool. If service level is not defined with the Call Type tool, but is defined with the System Information tool, the Unified CCE uses the System Information setting.

**Service level type.** Indicates how the system software calculates the service level for the service. The default is the level specified for the associated peripheral. To set a different level type, check the **Override System Information Default** check box and select the type you want from the selection box.

**Bucket Intervals.** Indicates the Bucket Intervals setting for the call type. Bucket intervals are defined with the Bucket Intervals List tool. If you wish to override the defined default, check the **Override System Information Default** check box and select a different Bucket Intervals setting.

**Description.** Enter an optional description of the call type.

**Step 4** 
Click **Save** to enter the call type information.

Repeat this procedure to add additional call types.

### Configure Variables

#### Configure Expanded Call Context Variables

Expanded Call Context (ECC) variables are variables that you define and enable in the Configuration Manager to store values associated with the call. You can specify the variable name and data type. The name must begin with the string "user." These are in addition to the variables the system software defines for each call (PeripheralVariable1 through PeripheralVariable10, CallerEnteredDigits, CallingLineID, and so on).

An ECC variable name can be up to 33 bytes long (1–32 usable characters). Use the following naming convention when creating an ECC variable:

`user.<CompanyName>.<VariableDescription>`

In this syntax:

- `<CompanyName>` is the name of your company
- `<VariableDescription>` is a descriptive tag for the variable.

For example, you could use the following name for an ECC variable created for Cisco account numbers:

`user.Cisco.AcctNum`

Using this naming convention prevents naming conflicts with any third-party applications that interface with the system software.

**Note**

If your corporation is large, you may want to break `<VariableDescription>` down to include the Business Unit, Division, or other organizational entity that exists in your company.

In addition:

- An ECC variable can be either a scalar variable or an array element, each with a maximum length of 210 bytes.
Array types are not supported for an agent request.

Note

• The maximum number of elements in an array can be 255.
• The maximum buffer size for each scalar variable = 5 + the maximum length of the variable where the 5 bytes includes 4 bytes to tag the variable and 1 byte for the null terminator.
• The maximum buffer size for each array = 5 + (1 + the maximum length of array element) * (the maximum number of elements in the array).
• There is a null terminator for each element, as well as a null terminator for the array as a whole.
• Since the total size of the buffer used to store the variables internally is 2000 bytes, the total sum of all the maximum buffer sizes for each variable and each array must be no greater than 2000.

For example, if you intended to use one scalar ECC variable with a maximum length of 100 bytes, one scalar ECC variable with a maximum length of 80 bytes, and an ECC array with a maximum of 9 elements with each element having a maximum length of 200 bytes, the buffer size would be: (5+100) + (5+80) + (5 + (1+200)*9) = 2004. As this buffer size is too large, the length of one of the scalar ECC variables or the length of the array ECC variable must be adjusted.

For Web Callback and Delayed Callback to work properly, an ECC variable (also known as a named variable) must be defined. The Cisco CTI driver supports the use of ECC variables in addition to the standard call variables associated with a call. Before an ECC variable can be used, it must be defined in the Unified CCE ECC variable database table.

ECC Variables for Blended Collaboration or Voice MRDs with Collaboration

ECC variables must be configured in Configuration Manager's Expanded Call Variable List tool (for each integrated application) to route requests using the voice Media Routing Domain.

For Cisco Blended Collaboration or Voice MRDs with Collaboration, the ECC variables are:

• user.cisco.cmb
• user.cisco.cmb.callclass
• user.cim.activity.id
• user.wim.customer.name

Important

While their default size is 40 characters, use the Expanded Call Variable List tool in the Configuration Manager to limit the user.cisco.cmb variable to 8 bytes and the user.cisco.cmb.callclass variable to 10 bytes to prevent ECC space limitation issues.

Validate ECC Variable Size for CTI Server

Before configuring ECC variables, validate the total size of the ECC variables against the following rules and limits:

• Because the total size of the buffer used to store the variables in CTI Server internally is 2500 bytes, the total sum of all the maximum buffer sizes for each scalar variable and arrays must be no greater than 2500.
• The maximum buffer size for each scalar variable = 4 + length of the ECC name + the maximum length of the variable where the 4 bytes includes a 1 byte tag, 1 byte to define the length, and 2 terminating NULL characters.

• The maximum buffer size for each array = (5 + length of the ECC name + the maximum length of array element) * (the maximum number of elements in the array) where the 5 bytes includes a 1 byte tag, 1 byte to define the length, 1 byte for the array index, and 2 terminating NULL characters.

• For example, if you intend to use one scalar ECC variable with a maximum length of 100 bytes named user:var, one scalar ECC variable with a maximum length of 80 bytes named user:vartwo, and an ECC array named user:varthree with a maximum of 9 elements with each element having a maximum length of 200 bytes, the buffer size would be:

\[(4+8+100) + (4+11+80) + ((5 + 13 + 200)*9)) = 2169\]

where 8 is the length of user:var, 11 is the length of user:vartwo and 13 is the length of user:varthree.

Enable ECC Variables

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Within the Configuration Manager, double-click <strong>Tools &gt; Miscellaneous Tools &gt; System Information</strong>. The System Information window appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the <strong>Expanded call context enabled</strong> check box. For additional information, refer to the online Help.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Save</strong> to apply your changes.</td>
</tr>
</tbody>
</table>

Define ECC Variables

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Within the Configuration Manager, double-click <strong>Tools &gt; List Tools &gt; Expanded Call Variable List</strong>. The Expanded Call Variable List window appears.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Expanded Call Variable List window, enable Add by clicking <strong>Retrieve</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Add</strong>. The Attributes property tab appears.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Complete the Attributes property tab:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong> (required)</td>
<td>The enterprise name of the expanded call variable. This name must start with the string user and must be unique among all expanded call variables in the system (an enterprise name).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Use the following syntax to prevent naming conflicts: user.company.name where company is your company name and name describes the expanded call variable.</td>
</tr>
</tbody>
</table>
**Maximum length (required)**

Specifies the maximum number of characters (1–210) allowed in the extended call variable value (the size of the variable string). For a numeric value, the number of digits is specified.

Important notes:

- The maximum amount of space that all the ECC variables together can take up in the Unified CCE system is no more than 2000 bytes (not 2K or 2048 bytes) and sometimes less, depending on your combination of scalar and array variables and their sizes. Each ECC variable takes up space based on the following formula: For scalar: 5 + Maximum_Length For array: 5 + (1 + Maximum_Length) * (Maximum_Array_Size)

- The number of characters or digits does not indicate the number of bytes. For example, a scalar ECC variable of 10 characters could take up 15 bytes of space.

**Array (check box)**

When selected, indicates the expanded call variable is an array, not a scalar. Maximum array size If the expanded call variable is an array, this indicates the maximum number of elements (1–255) in that array. See also the note under the Maximum length description. Note: Arrays are not supported with the Agent Request feature.

**Enabled (check box)**

When selected, the expanded call variable is included for each call.

**Persistent (check box)**

When selected, ECC variables are written to the Logger database.

**Note**

Non-persistent variables can be used in routing scripts, but are not written to the database. Because these variables may be persisted, do not use ECC variables to store sensitive information belonging to the customer or company. Storing confidential information in these variables can lead to violation of security standards, such as PCI, the Common Criteria, HIPAA, or FIPS 140-2.

**Cisco provided (check box)**

When selected, indicates that the system software predefines the selected expanded call variable.

**Description**

Provides additional information about the ECC variable.

**Step 5**

Click **Save** to apply your changes.

---

**Configure User Variables**

You can also create global user variables; for example, you can create a user variable called usertemp to serve as a temporary storage area for a string value used by an If node.

After you have defined a user variable, you can then use the Script Editor Formula Editor to access the variable and reference it in expressions, just as you would with a "built-in" variable.

Each user variable must:

- Have a name that begins with user.
This name cannot contain the dot/period (.) character.

- Be associated with an object type, for example, Service. (This enables the system software to maintain an instance of that variable for each object of that type in the system.)

- Be identified as a persistent (retains value across CallRouter restarts) or non-persistent (does not retain value across CallRouter restarts) variable.

Note Because these variables may be persisted, do not use User Variables to store sensitive information belonging to the customer or company. Using these variables to store confidential information could lead to violation of security standards, such as PCI, the Common Criteria, HIPAA, or FIPS 140-2.

A user variable can store a value up to 40 characters long.

**Define User Variables**

**Procedure**

**Step 1** Within the Configuration Manager, select Tools > List Tools > User Variable List.
The User Variable List window appears.

**Step 2** In the User Variable List window, click Retrieve to enable Add.

**Step 3** Click Add.
The Attributes property tab appears.

**Step 4** Complete the Attributes property tab.

Note The Variable name, Object type, and Data type fields are required. All other fields are optional.

For additional information refer to the online Help.

**Step 5** Click Save to apply your changes.

**Configure Users**

**Create Person records**

All Unified CCE agents must have a Person record. When you create an Agent record, you can associate the record with an existing Person record. If you do not associate the Agent record with an existing Person record, a new Person record is automatically created when you create the agent.

To configure a Person record before configuring an agent, complete the following steps:

**Procedure**

**Step 1** From the Configuration Manager, choose Peripherals > Person > Person List.
The Person List dialog box opens.

**Step 2** Click **Retrieve** and then click **Add**.

**Step 3** in the Attributes tab, enter information in the following fields:
- **First Name.** Enter the person's first name.
- **Last Name.** Enter the person's last name.
- **Login Name.** Enter the person's login name.
- **Password.** Enter a password for the person.
- **Enable Logins.** Check this check box.

**Step 4** Click **Save** and then click **Close**.

**Step 5** Repeat this procedure to add additional Person records.

---

**Associate agents with peripherals**

**Procedure**

**Step 1** Select **Tools > Explorer Tools > Agent Explorer**.
The Agent Explorer dialog box displays.

**Step 2** Select the peripheral you want associated with the agent from the drop-down list and click **Retrieve**.

**Step 3** Click **Add Agent** to display the Agent configuration tab.

**Step 4** In the Agent tab, enter information in the following fields:
- **Last Name.** Enter the agent's last name.
- **First Name.** Enter the agent's first name.
- **Login Name.** Enter the name the agent uses to login. This name must be unique in the enterprise.
- **Password.** Enter the agent's password. This password is validated during the agent login process.
- **Login Enabled.** Check this check box if you want the enable the agent to login.
- **Select Person.** Click this button to select a person to associate with the agent record. You can select a person for a new agent, an existing agent, or a temporary agent.
- **Enterprise Name.** Enter an enterprise name for the agent that is unique within the enterprise. The default is a combination of the peripheral name with the agent's first and last name.
- **Peripheral Name.** Enter a name for the agent as known to the peripheral.
- **Peripheral Number.** Enter the agent's login ID. This number identifies the agent to the peripheral. This number needs to be unique among all agents for the peripheral, but does not need to be unique across all peripherals. Agent IDs can be up to nine digits long. The first digit in the ID must be 1 through 9. It cannot be 0. Also, this number cannot be the same as the extensions on the Unified Communications Manager cluster for this agent. Finally, the ID cannot exceed the extension length specified in the Unified Communications Manager Peripheral Gateway Setup.

**Step 5** Click the Advanced tab and enter information in the following fields:
- **Desk Setting.** Use the drop-down list to select the desktop settings to be associated with the agent. If you do not make a selection, the Unified CCE applies the default desk settings defined for the peripheral.
**Assign Agent Desk Settings**

Agent Desk Settings associate a set of permissions or characteristics with specific agents. The settings are comparable to Class of Service settings on a PBX or ACD. Desk settings are associated with an agent when you configure the agent. The desk settings are global in scope and you can apply them to any configured agent on any peripheral within a Unified CCE configuration.

Agent Desk Settings provide a profile that specifies parameters such as whether auto-answer is enabled, how long to wait before rerouting a call for Ring No Answer, what DN to use in the rerouting, and whether reason codes are needed for logging out and going not-ready. You must associate each agent with an agent desk setting profile in the Unified CCE configuration. A single agent desk setting profile can be shared by many agents. Changes made to an agent's desk setting profile while the agent is logged in are not activated until the agent logs out and logs in again.

If Agent Desk Settings are not associated with an agent, the agent is assigned the peripheral default settings, which depend on the peripheral to which the agent is assigned.

When you configure Agent Desk Settings, you specify the amount of non-active time after which an agent is automatically logged out, whether wrap up is required following incoming and outbound calls, the amount of time allocated for wrap up, and the method used for assist and emergency calls. You also specify settings for the Ring No Answer feature.

**Ring No Answer**

The Ring No Answer feature, configured in Agent Desk Settings, ensures that when an agent does not answer a call, the call is taken away from the agent after a specified number of seconds and re-assigned to another agent or requeued.

When a call is routed to an agent but the agent fails to answer the call within a configurable amount of time, the Unified Communications Manager PIM for the agent who did not answer changes that agent's state to not ready (so that the agent does not get more calls) and launches a route request to find another agent. Any call data is preserved and popped onto the next agent's desktop. If no agent is available, the call can be sent back to the Unified IP IVR for queuing treatment again. Again, all call data is preserved. The routing script for this RONA treatment should set the call priority to “high” so that the next available agent is selected for this caller. In the agent desk settings, you can set the RONA timer and the DN used to specify a unique call type and routing script for RONA treatment.

This feature behaves and is configured differently depending on whether you deploy the Unified CVP or Unified IP IVR in the Unified CCE System.
The Dialed Number for Ring No Answer is peripheral-specific. Therefore, each Unified Communications Manager PG in your deployment must have its own set of Agent Desk Settings configured for it; you cannot use a particular desk setting across peripherals.

About Ring No Answer with Unified IP IVR

For Unified CCE systems in which you deploy the Unified IP IVR, the Ring No Answer feature ensures that when an agent does not answer a call the following applies:

- The call is taken away from that agent after ringing for a configurable number of seconds and is rerouted to a different agent or placed in queue.
- The state of the agent who did not answer the call is changed to "Not Ready."

Reroute a call on Ring No Answer works as follows for Unified IP IVR:

1 A routing script connects the call to an agent.
2 If the agent does not answer the phone within the Ring No Answer time set in Agent Desk Settings, the Unified Communications Manager changes the agent's state to "Not Ready" and post routes the call to Unified CCE.
3 The Unified CCE Router runs a routing script using the dialed number specified in the agent desk setting record. The routing script associated with the DN typically looks for another agent and routes the call to that new agent.
4 If no agents are available, the call typically is translation routed or queued to the VRU, or sent to some other queue point. Queuing treatment is restarted.

Note
Give the call the highest priority in the queue so that the call is routed to the next available agent.
5 Any call data is preserved to be popped onto the agent screen. In addition, a flag is set in the database so that Unified CCE can report on all of the occurrences of Ring No Answer.

About Ring No Answer with Unified CVP

For Unified CCE systems in which you deploy the Unified CVP, the Unified Communications Manager does not control the Unified CVP and cannot send an unanswered call back to the Unified CVP for re-queuing. You configure the Ring No Answer feature to only make the agent “Not Ready” when they do not answer a call, and use the Unified CVP Router Requery feature to re-queue the call.

As of Release 9.0, the Unified CVP deployment no longer requires that you configure the RNA timer on both sides (Unified CVP and Unified CCE); configure Ring No Answer (RNA) timeout only in Unified CVP. This removes the requirement to manually align the relevant Unified CVP and Unified CCE timer configuration. To configure RNA timeout in Unified CVP, see the Patterns for RNA timeout on outbound SIP calls section in the Unified CVP OAMP console.

Reroute a call on Ring No Answer works as follows for Unified CVP:

1 A routing script connects the call to an agent by sending a connect message to the Unified CVP. The script node should have Enable Target Requery enabled. To enable this, edit the node, select Change and check the Enable Target Requery check box.
2 The agent's phone rings.

3 If the phone is not answered (either via the agent desktop or physically going off-hook) within the Ring No Answer time set in Agent Desk Settings, Unified CCE makes the agent unavailable, but does not actually change the agent state to Not Ready until the call is redirected.

4 When the Unified CVP Ring No Answer timeout expires, the Unified CVP sends an EventReport=No Answer message to the Router instructing it to select another target according to the routing script and send a Connect message to Unified CVP. The target might be another agent or a VRU label to requeue the call.

Note Give the call the highest priority in the queue so that the call is routed to the next available agent.

5 Any call data is preserved to be popped onto the second agent screen.

Note In addition, a flag is set in the database so that Unified CCE can report on all of the occurrences of Ring No Answer.

6 When the call is redirected from the original agent, the agent's state changes to “Not Ready.”

Configure Agent Desk Settings

Procedure

Step 1 From the Configuration Manager, choose Configure ICM > Enterprise > Agent Desk Settings > Agent Desk Settings List. The Agent Desk Settings List dialog box opens.

Step 2 Click Retrieve and then Click Add.

Step 3 Fill in the Attributes tab information:

Name. Enter a name for the agent desk settings that is unique within the enterprise.

Ring No Answer Time. Enter the number of seconds (between 1 and 120) that a call may ring at the agent's station. If you are deploying the Unified CVP, make sure this number is less than the number set for the No Answer Timeout for Router Requery that you set in the Unified CVP.

If you configure this timer, you do not need to configure the Unified Communications Manager Call Forward on No Answer for agent extensions in the Unified Communications Manager, unless you want them to be used when the agent is not logged in. If you set the Unified Communications Manager Call Forward No Answer time, enter a value at least 3 seconds higher than the Ring No Answer Time on each Unified Communications Manager node.

Ring no answer dialed number. Enter the Unified CCE DN associated with the routing script that you want to use to reroute a call that an agent has not answered. If you are deploying the Unified CVP, leave this field blank.

Logout non-activity Time. Enter the number of seconds (between 10 and 7200) in which the agent can remain in Not Ready state before Unified CCE automatically logs out the agent.

Work Mode on Incoming. Select whether wrap-up is required following an incoming call. Select an option from the drop-down list.
Work Mode on Outgoing. Select whether wrap-up is required following an outgoing call. Select an option from the drop-down list.

Wrap Up Time. Enter the amount of time, in seconds, allocated to an agent to wrap up a call.

Assist Call Method. Select whether Unified CCE creates a consultative call or a blind conference call for a supervisor assistance request.

Emergency Alert Method. Select whether the Unified CCE creates a consultative call or a blind conference call for an emergency call request.

Blind conference is not supported if the call may queue on a VRU.

Description. Enter additional optional information about the agent desk settings.

Step 4 Use the following boxes to select or de-select miscellaneous settings:

Auto-answer. Indicates whether calls to the agent are automatically answered. The agent is not required to take any action to answer the call. If a second call comes in while a call is in progress, the call is not automatically answered. This is the same behavior as with Unified Communications Manager.

If you enable auto-answer, you must also configure the agent phone in Unified Communications Manager to turn the speakerphone or headset (or both) to ON. If you turn only the headset to ON, the agent must also turn the phone headset button to ON.

In a multi-line enabled environment with auto-answer selected, if you are on a call on your non-ACD line, the call will not auto-answer. However, if you turn on Unified Communications Manager Auto Answer, the call will answer.

Idle Reason Required. Indicates whether an agent is required to enter a reason before entering the Idle state.

Logout Reason Required. Indicates whether an agent is required to enter a reason before logging out.

Auto Record on Emergency. Indicates in a record request is automatically sent when an emergency call request starts.

Cisco Unified Mobile Agent (check box). Enables the Unified Mobile Agent feature so that the agent can log in remotely and take calls from any phone. For more information about the Unified Mobile Agent, see the Cisco Unified Contact Center Enterprise Features Guide at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.html.

Step 5 Click Save and then click Close.

Designate agent supervisors

When you create an agent, you can assign that agent to be an agent supervisor.

Procedure

Step 1 On the open Agent Explorer for the agent that you want to make a supervisor, click the Supervisor tab.

Step 2 On the Supervisor tab, enter information in the following fields:

Supervisor Agent. Check this check box to indicate that the selected agent is a supervisor.

Domain name. Select the trusted domain name from the drop-down list. The location button when selected, lists the Active Directory folders in the selected domain.

Supervisor login as user. Enter the Active Directory user ID of the selected agent.
If you enter an existing user from the domain in the edit box, a message appears stating: "The account <name> in domain <domain name> exists. Do you want to associate an agent supervisor with this existing account?" If you select "Yes," the agent supervisor is associated as a Unified CCE user. If you select "No," you must enter a name again.

If the user does not exist, the user is created on the domain.

Note A single user with Configuration Manager credentials cannot be defined as both a "Supervisor" and a "Unified ICM/CCE/CCH user". The following error occurs in such case: "User XXX in YYY Domain exists as an ICM user or is already a Supervisor. Please select another user." To circumvent this limitation, create two records for this user with the same basic username, but with a different role appended to each (for example, for user1 create user1.supervisor and user1.icm).

A user who is defined as a supervisor agent can access and use the Supervisor Desktop, CCE Web Administration Tool. Supervisors can also add and remove members of their teams.

**Supervisor login password.** Enter the Active Directory User password for the account of the selected supervisor agent.

**Description.** Enter an optional description for the supervisor.

**Create agent teams**

You can group individual agents into agent teams that supervisors can manage. Agent teams are assigned to specific peripherals, so you must assign all agents of a given team to the same peripheral. You assign agents individually to agent teams.

When configuring agent teams, be aware of the following rules:

- An agent can be a member of only one agent team.
- An agent team can have only one Primary Supervisor.
- A supervisor can be a supervisor of any number of agent teams.
- A supervisor for an agent team can also be a member of that agent team.
- All agents belonging to an agent team and all supervisors for that agent team must be on the same peripheral.

For more information on team limits, see the appendix on system requirements in the *Cisco Unified Contact Center Enterprise Design Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

**Procedure**

**Step 1** From the Configuration Manager, select **Configure ICM > Peripherals > Agent Team > Agent Team List.**

**Step 2** Click **Retrieve** and then **Add** to add a new agent team.

**Step 3** Click the **Attributes** tab and enter values in the following fields:

- **Name.** Enter an enterprise name for the agent team that is unique within the enterprise.
- **Peripheral:** Enter the name of the agent team peripheral. You can select the name from the drop-down list.
Supervisor Script Dialed Number: Select a dialed number for the agent team from the drop-down list. If you have not created a supervisor script, select the default, “none”. When you create the script, return to this screen and enter the dialed number for the script.

Description: Enter additional information about the agent team.

Step 4 Click the Members tab and click Add.
Step 5 Choose the agents that you want to assign to the team and click OK.
Step 6 Click the Supervisor tab and choose the supervisor from the Primary Supervisor drop-down list.
Step 7 To add a secondary supervisor, click the Add button and select a secondary supervisor from the list. Click OK.
Step 8 Click Save and then click Close.

Configure Network VRUs

Use the Configuration Manager tool to configure Network VRUs.

After you configure a Network VRU and VRU scripts, you can use the Script Editor to write a routing script to send a call to the VRU and invoke a specific VRU script.


Create Network VRU Target

Procedure

Step 1 Within the Configuration Manager, select Tools > Explorer Tools > Network VRU Explorer. The Network VRU Explorer window appears.
Step 2 In the Network VRU Explorer window, click Retrieve to enable Add Network VRU.
Step 3 Click Add Network VRU. The Network VRU property tab appears.
Step 4 Complete the Network VRU property tab. The Name and Type fields are required. All other fields are optional. For additional information refer to the online Help.
Step 5 Click Save to apply your changes.

Define Network VRU Label

You must associate all VRU Types (except Type 6) with a Network VRU label.
Procedure

**Step 1**  
In the Network VRU Explorer window, click **Retrieve** and select the Network VRU you want to add the label to.  
The Label property tab appears.

**Step 2**  
Complete the Label property tab.  
The **Routing client**, **Label**, and **Label type** fields are required. All other fields are optional. For additional information refer to the online Help.

**Step 3**  
Click **Save** to apply your changes.

Set Default Network VRU and Range of Correlation Numbers

For Network VRUs, you must use the System Information dialog to define a range of correlation IDs so the system software can communicate with the VRU about the call.

Procedure

**Step 1**  
Within the Configuration Manager, select **Tools > Miscellaneous Tools > System Information**. The System Information window appears.

**Step 2**  
In the System Information window, select the **Default Network VRU**.

**Step 3**  
Enter the **Minimum Correlation Number**.

**Step 4**  
Enter the **Maximum Correlation Number**.  
For additional information refer to the online help.

**Step 5**  
Click **Save** to apply your changes.

Configure scripts

**Network VRU scripts**

*VRU scripts* differ from routing scripts. A configured VRU script runs only when the Unified CCE instructs it to do so from a routing script. A VRU script on the Unified CCE is the configured record for the VRU script that resides on the VRU system. A VRU script executes to collect digits, play hold music, or perform many other common functions.

After you configure the VRU scripts, you can use the Script Editor to write a routing script to send a call to the VRU and invoke a specific VRU script.

For deployments that include the Unified CVP, use the Translation Route to VRU node to send calls to the Network VRU and invoke VRU scripts. Do not use Translation Route to VRU node for deployments that use the Unified CCE System PG. Instead, use any one of Queue to Skill Group or Send to VRU nodes.
Routing and administrative scripts

A routing script processes call routing requests from a routing client. Typically it examines several targets and applies selection rules to find an available qualified agent or a target with the shortest expected delay. You can set up different routing scripts to execute for different types of tasks. You can define call types in terms of the telephone number the caller dialed, the number the caller is calling from, and additional digits entered by the caller. For each call type, you can schedule different routing scripts to execute on different days or at different times of the day.

An administrative script runs periodically to perform a task, such as setting variables.

Configure Network VRU scripts

Procedure

Step 1 From the Configuration Manager, select Tools > List Tools > Network VRU Script List. The Network VRU Script List dialog box opens.

Step 2 Click Retrieve and then click Add.

Step 3 On the Attributes tab, enter the configuration information for the VRU script as follows:

**Network VRU**. Specify the Network VRU with which this script should be associated.

**VRU Script Name**. Enter script name; for example, BasicQ.

**Name**. Enter the script file name; for example, BasicQ.aef

**Timeout [seconds]**. Enter 180.

**Configuration param**. Leave blank.

**Customer**. Choose the same Unified CCE customer you chose for call type from the drop-down list.

Step 4 Check the **Interruptible** check box.

Step 5 Click **Save** and the click **Close**.

Troubleshoot Network VRU scripts

If a timeout occurs on a VRU script, it is possible that the Router does not notify the VRU PIM that a timeout has occurred. Because the VRU PIM is not informed of the problem, it does not notify the VRU to cancel the script.

At this point, the options for script flow include the following:

- The failure path in the Router script sends the call to a label, the VRU PIM gets a Connect and, if the VRU supports it, generates a Cancel message. This is the most common result.

- Before the Router picks a label, the VRU script completes and the VRU sends a Script Result message to the Router. The Router then sends a Dialogue Failure Event because it is not expecting a Script Result. This is the next most common result.

- The failure path in the Router script tries to run another VRU script. This is not a common result.
Currently, the best resolution to this problem is to use longer time-outs or create shorter VRU scripts. Be aware that the failure exit from the Run VRU Script node is a problem that you may need to resolve.

**VRU error checking**

A special call variable VruStatus, allows you to check the result of the last VRU node (Send To VRU/Translation Route to VRU/Run VRU Script) that the Unified CCE processed. The following table lists the values for this variable.

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>VRU_SUCCESS</td>
<td>The last VRU node was successful.</td>
</tr>
<tr>
<td>1</td>
<td>VRU_ERROR</td>
<td>The last VRU node failed because of a routing or configuration error.</td>
</tr>
<tr>
<td>2</td>
<td>VRU_TIMEOUT</td>
<td>The last Send To VRU or Translation Route to VRU node failed because the routing client did not respond within 20 seconds or the last Run VRU Script node failed because the timeout limit defined for the script expired.</td>
</tr>
<tr>
<td>3</td>
<td>VRU_ABORTED</td>
<td>The last VRU node did not complete because the caller hung up or was otherwise lost. (Because this causes the routing script to terminate immediately, this value is never seen.)</td>
</tr>
<tr>
<td>4</td>
<td>VRU_DIALOG_FAILED</td>
<td>The last VRU node failed because communication with the VRU ended unexpectedly.</td>
</tr>
<tr>
<td>5</td>
<td>VRU_SCRIPT_NOT_FOUND</td>
<td>The VRU failed because the referenced VRU script was not found in the Unified CCE configuration.</td>
</tr>
</tbody>
</table>

**Configure routing and administrative scripts**

After you complete your Unified CCE configuration, you can write routing scripts and administrative scripts. You create, maintain, and monitor these scripts using the Script Editor.

<table>
<thead>
<tr>
<th>For Information about</th>
<th>See</th>
</tr>
</thead>
</table>
Configure Agent or Device Targets

**Note**
Device targets are deprecated. Use Agent Targeting Rules instead.

Configure Agent Targeting Rules

The Agent Targeting Rules (ATR) configures call routing by specifying the agent extension range, instead of configuring Device Targets and Labels for every phone/Routing Client. This simplifies the call routing configuration for the Agent PGs. Also, this feature reduces the amount of memory used by the Router because a large number of Device Targets and Labels are replaced by a few rules. ATRs are therefore, the preferred method for installation.

**Before You Begin**
You must configure the PGs and routing clients before you configure the Agent Targeting Rules.

**Procedure**

**Step 1**
From the Configuration Manager, choose one of the following:
- Configure ICM > Targets > Device Target > Agent Targeting Rule.
- Tools > List Tools > Agent Targeting Rule.

The ICM Agent Targeting Rules dialog box opens.

**Step 2**
Click Retrieve.

**Step 3**
Click Add.

**Step 4**
Enter a name for the rule.

**Step 5**
Select a peripheral where the rule will be associated.

**Step 6**
Select the rule type:
- Agent Extension
- Substitute Agent Extension: Enter the agent extension prefix and agent extension length.
- Translation Route: Select a Translation Route.
For the Translation Route option, you must also configure the Translation Route DAIS as dialed numbers associated with the target agent's peripheral routing client in Unified CCE. You must map the dialed numbers to the route points that are configured in Unified Communications Manager and associated with the JTAPI user. This is necessary to complete the Translation Route Rule.

Step 7 Select one or more routing clients that can initiate the route request.

Step 8 Enter the agent's extension range.

Step 9 Click Save.

Step 10 Test the rule configuration by routing calls from each routing client to each agent extension you defined. If you defined a range, simplify the test by testing the lower and the upper limits of the agent extension, and a sampling of the extensions in between the range limits.

Configure device targets and labels

Note

Device targets are deprecated. Use Agent Targeting Rules instead.

A device target is a telephony device that can be uniquely addressed by a telephone number. If you use device targets, you configure a device target for each IP telephone that an agent uses. A device target is not associated with any one peripheral. Each device target must have one or more associated labels, although only one label may exist per routing client. The Unified CCE uses the device target to locate the label that routes a call to a Unified CCE agent.

An agent is dynamically associated to a device target at the time the agent logs in to a peripheral. The agent log-in request specifies the device target, or targets, to be associated with the agent. The association between the agent and the device target lasts until the agent logs out of the peripheral.

After you configure device targets, you can verify that you have configured agents properly in the Unified CCE by placing an Agent to Agent call. This test verifies your installation and configuration of the JTAPI client, CTI OS, and agents in the Unified CCE. To verify agent configuration, you must log in as an agent and then make a call to another agent. Calling another agent requires that you use the agent ID and not the phone number of the instrument.

You configure each IP phone in the Unified CCE as a device target. You can configure only one extension on the phone as a device target. You can configure additional extensions on the phone, but Unified CCE does not operate with those extensions. So, no monitoring or control of those additional extensions is possible. Unified CCE provides call treatment for ring no answer (RONA). So, you do not configure call forwarding on ring-no-answer in the Unified Communications Manager configuration for the phones. Unless call center policy permits warm (agent-to-agent) transfers, the Unified CCE extension also should not be published or dialed by anyone directly, and only Unified CCE should route calls to this phone extension.

At agent login, the agent ID and phone extension are associated, and this association is released when the agent logs out. This feature allows the agent to log in to any agent phone. At agent login, the Unified Communications Manager PIM requests the Unified Communications Manager to begin monitoring the agent phone and to provide device and call control for that phone. Each phone must be mapped to the Unified CCE JTAPI user ID in order for the agent login to be successful.
Configure device targets

**Note** You do not have to configure device targets if your deployment uses a Unified CCE System PG. Device targets are deprecated. Use Agent Targeting Rules instead.

**Procedure**

**Step 1** From the Configuration Manager, select Configure ICM > Targets > Device Target > Device Target Explorer.

The Device Target Explorer window opens.

**Step 2** Click Retrieve and then click Add Device Target.

The Device Target tab opens.

**Step 3** In the Device Target tab, enter values in the following fields:

- **Name**: Enter an enterprise name for the target. This name must be unique among all device targets in the enterprise.
- **Global Address**: A unique identifier. The global address can be any unique string.
- **Config Parameters**: Use this field to enter any specific configuration parameters you may require:
  - `/devtype` (CiscoPhone)
  - `/dn` (full phone number) /`ext` (extension)

The Unified CCE gives this string to the Unified Communications Manager to initialize the device.

Using the extension (ext) may be optional, depending on your environment. In most cases, using the dialed number (DN) is sufficient. The DN must start with a number 1 through 9 (0 is not allowed), and the extension length must match the length that you indicated in the Unified Communications Manager Peripheral Gateway Setup.

- **Description**: Enter a description of the device. This is an optional field used to provide additional information about the device.

**Step 4** Click Save.

Configure labels

**Note** If your deployment uses a Unified CCE System PG, you do not have to configure labels.

**Procedure**

**Step 1** In the Device Targets Explorer window, select the target (service) for which you are creating the label and click Add Label.

**Step 2** In the Label tab, enter values in the following fields:
**Routing Client.** Select the enterprise name of the routing client that can receive the label. Configure a label for each type of Unified CCE routing client, including the interexchange carriers, NICs, Network VRUs, and post-routing PGs.

**Label.** Enter the literal string of characters to be returned to the routing client.

**Label Type.** Enter the label type. The label type for the Unified CCE is Normal.

**Customer.** Choose the customer (Unified CCE Instance) from the drop-down list.

**Description.** Enter optional information about the label.

**Step 3** Click **Save**.

The Unified CCE generates a unique value for the Label Name list after you save the attributes. Repeat this procedure for any additional labels.

---

**Configure translation routes**

Use the Translation Route wizard to configure the translation routes for the Unified Communications Manager and VRU peripherals. This wizard automates the correct associations with peripheral targets, labels, and routes.

---

**Note**

Run the Translation Route Wizard only if your Unified CCE solution uses Unified CVP.

---

**Procedure**

**Step 1** In the Configuration Manager, select **Tools > Wizards > Translation Route Wizard**.

The Translation Route Wizard introductory dialog box opens.

**Step 2** Click **Next**.

The Acquire Lock and Select Configuration Task dialog box opens.

**Step 3** Select **Create New**.

**Step 4** Click **Next**.

The Define Translation Route dialog box opens. The graphic on the left of the dialog box shows the entities you are defining while using the Translation Route Wizard.

**Step 5** Enter a long and short name for the translation route and, optionally, a description (the short name is used in forming target names).

**Step 6** Click **Next**.

The Select Configuration dialog box opens.

**Step 7** Choose the single peripheral, single routing client configuration from the drop-down list.

The graphic changes to show the configuration you select.

**Step 8** Click **Next**.

The Select Peripheral Gateway, Peripherals, and Services dialog box opens.

**Step 9** Enter values for the following fields:

- **Peripheral Gateway.** Choose the gateway target for the translation route.
Peripheral. Choose the single peripheral or the peripheral to route calls to.

Service/Service Array. If the translation route is associated with a single peripheral, choose the service associated with the translation route. If the translation route is associated with multiple VRUs, then select a service array.

Step 10 Click Next. The Select Routing Clients and Dialed Numbers dialog box opens. Use this dialog box to specify the Unified Communications Manager peripheral (or VRU peripheral) as the routing client from which translation routed calls originate. For the Unified CCE the dialed number string is not applicable.

Step 11 Click Next. The Select Network Trunk Groups for Routing Clients dialog box opens. Choose at least one network trunk group to be used in peripheral targets associated with the translation route.

Step 12 Choose a routing client, select a network trunk group value for it, and click Add. The Network Trunk Group appears in the list at the bottom of the dialog box.

Step 13 Click Next. The Configure DAIS dialog box opens.

Step 14 Use this dialog box to specify the DAIS values that map to route points on the VRU. Do one of the following:

- To enter a specific DAIS value, click Add DAIS and enter the value.

- To add a range of DAIS values, typically required by a translation route, click Add DAIS Range.

A dialog box prompts you to enter a starting and ending DAIS value. The Translation Route Wizard automatically generates the DAIS values in the range.

Step 15 Click Next. The Configure Label dialog box appears.

Step 16 Use this dialog box to define a label that maps to the DAIS/CTI route points. A label consists of a prefix and a suffix. Each DAIS value requires a unique label. Do one of the following:

- Enter prefixes and suffixes individually.

- Use the buttons in this dialog box to set a range of values or to base the prefix or suffix values on the DAIS values.

Step 17 Click Next. The Wizard Complete dialog box opens.

Step 18 Click Create Translation Route to create the translation route and its associated entities. First, the Translation Route Wizard displays a success message and then the dialog box appears.

Step 19 Do one of the following:

- To see details about the translation route you just created, click Run Report.

- To return to the beginning of the Translation Route Wizard and perform a new task, select Start New Task and click Finish.
- To exit the Translation Route Wizard, click **Finish**.

**Note**

You can also use the Translation Route Explorer to create a translation route or to modify a translation route that you created with the Translation Route Wizard. Select **Configuration Manager > Tools > Explorer Tools > Translation Route Explorer**.

**Configure Skill Groups or Precision Routing**

Skill groups are collections of agents that share a common set of skills. Skill groups are associated with a peripheral and are members of Services. You can associate agents with one or more skill groups.

To configure skill groups, you create skill groups, add the skill groups to services as members, and assign agents to one or more skill groups.

Precision routing offers an alternative to skill group routing. Using Unified CCE scripting, you can dynamically map the precision queues to direct a call to the agent who best matches the precise needs of the caller.

To configure precision routing, you create attributes, assign attributes to agents, create precision queues, and create routing scripts.

**Configure Skill Groups**

**Add skill groups**

You configure skill groups to group agents with similar skills. You can associate agents with one or more skill groups. Skill groups are associated with a specific Unified Communications Manager PIM. You can group skill groups from multiple PIMs into Enterprise Skill Groups. You can direct calls to (routed to) Enterprise Skill Groups to share the load across multiple call centers or Unified Communications Manager installations. You can do reporting on Enterprise Skill Groups.

Agents are assigned one or more skills by associating the agent with the desired skill group.

After you create services and skill groups, you associate one or more skill groups with a service by making them members of that service.

A default skill group is created automatically when you create system PGs. The default skill group acts as a bucket to capture information about calls not routed by Unified CCE. (A call placed directly to an agent extension is an example of such a scenario.) If you deploy multichannel applications in your Unified CCE system, default skill groups are created for each Media Routing Domain that you configure.

**Note**

An agent must be assigned to at least one skill group to log in.

**Procedure**

**Step 1**

From the Configuration Manager, select **Configure ICM > Peripherals > Skill Group > Skill Group Explorer**.
The Skill Group Explorer dialog box opens.

Step 2 In the Select filter data section, select the peripheral from the drop-down list:

Step 3 Click Retrieve and then click Add Skill group to add a new skill group for the selected peripheral.

Step 4 Click the Skill Group tab and enter values for the following:


- **Peripheral Number**: Enter the skill group number as known by the peripheral. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.

- **Peripheral Name**: Enter the local name for the skill group. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.

- **Name**: The Configuration Manager generates the value for this field. This value is a unique name for the skill group made up of a default value from the peripheral enterprise name and the skill group peripheral name.

- **Available Holdoff Delay**: For the Unified CCE peripheral type, set this field to 0.

- **Priority**: This field is read-only and defaults to 0.

- **Extension**: Leave blank for the Unified CCE peripheral type.

- **ICM picks the agent**: Check this checkbox.

Step 5 Click Save and then click Close.

Step 6 Repeat this procedure for any additional skill groups.

---

**Assign skill groups as service members**

To make a skill group a member of a service, you establish mappings of skill groups to services. Each skill group can be mapped to zero, one, or more services. Each service can have zero, one, or more skill group members.

**Procedure**

Step 1 From the Configuration Manager, choose Configure ICM > Peripherals > Service > Service Explorer. The Service Explorer dialog box opens.

Step 2 Click Retrieve.

Step 3 Click the service that directs the skill group and then click the Service Members tab.

Step 4 On the Service Members tab, click Add to associate a skill group with the service.

Step 5 Click OK.

Step 6 Click Save and then click Close.

Step 7 Repeat this procedure for each skill group you want to associate with a service.

---

**Assign agents to skill groups**

Agents must be assigned to at least one skill group in order to log in. You can assign agents to the most appropriate skill groups according to their talents and skills to ensure that the most appropriate agent for a request responds to the customer.
Procedure

**Step 1**
From the Agent Explorer dialog box, choose the **Skill Group Membership** tab.

**Step 2**
From the Skill group name list, select the skill groups to which you want this agent assigned.

**Step 3**
Click **Add**.
The Add Skill Group Membership box opens, showing the skill groups to which the agent has been assigned.

**Step 4**
Click **OK**.

**Step 5**
Click **Save** and then click **Close** on the Agent Explorer dialog box.

**Step 6**
Repeat this procedure to assign additional agents to skill groups.

---

**Note**
You can remove agents from the Skill Group tab if necessary by selecting the agent and clicking **Remove**, then **Save**.

### Configure Precision Routing

To configure precision routing, use the Unified CCE Web Administration application, which links to various precision routing gadgets. To access the application, click the **CCE Web Administration** shortcut on your desktop, or copy the following URL into your browser: `https://distributor ip/ccadmin`.


### Add Attributes

**Procedure**

**Step 1**
Navigate to **Unified CCE Administration Manage > Attributes**.

**Step 2**
In the **List of Attributes** window, click **New**.

**Step 3**
Complete the following fields on the **General** tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>yes</td>
<td>Type a unique attribute name. For example, to create an attribute for mortgage insurance, type <em>mortgage</em>.</td>
</tr>
<tr>
<td>Description</td>
<td>no</td>
<td>Enter a maximum of 255 characters to describe the attribute.</td>
</tr>
<tr>
<td>Type</td>
<td>no</td>
<td>Select the type: Boolean or Proficiency.</td>
</tr>
<tr>
<td>Default</td>
<td>no</td>
<td>Select the default (True or False for Boolean, or a number from 1 to 10 for Proficiency).</td>
</tr>
</tbody>
</table>
Search for Agents

The Search field in the Agents tool offers an advanced and flexible search. Click the + icon at the far right of the Search field to open a popup window, where you can:

- Select to search for agents only, supervisors only, or both.
- Enter a username, agent ID, first or last name, or description to search for that string.
- Enter one or more team names separated by spaces. (Team is an OR search--the agent or supervisor must be a member of one of the teams.)
- Enter one or more attribute names separated by spaces. (Attributes is an AND search--the agent or supervisor must have all attributes.)
- Enter one or more skill group names separated by spaces. (Skill Groups is an AND search.)
- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**. Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Departments is an OR search.)

**Note** Search by department is enabled only when departments are configured.

Assign Attributes to Agents

**Procedure**

**Step 1** With the selected agent displayed, click the **Attributes** tab.

**Step 2** Complete the **Attributes** tab:
- This tab shows the attributes associated with this agent and their current values.
- Click **Add** to open a popup list of all attributes, showing the name and current default value for each.
  - Click the attributes you want to add for this agent.
  - Set the attribute value as appropriate for this agent.

Add Precision Queue

**Procedure**

**Step 1** Navigate to **Unified CCE Administration > Manage > Precision Queues**.
This opens a **List of Precision Queues** window showing all precision queues that are currently configured.

**Step 2**  
Click **New** to open the **New Precision Queue** window. Complete the fields.

<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>no</td>
<td>Enter up to 255 characters to describe the precision queue.</td>
</tr>
</tbody>
</table>
| Service Level Type    | yes      | Select the service level type used for reporting on your service level agreement.  
Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation.  
  
• **Ignore Abandoned Calls**  
  (the default): Select this option if you want to exclude abandoned calls from the service level calculation.  
  
• **Abandoned Calls have Negative Impact**: Select this option if you want only those calls that are answered within the service level threshold time to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level threshold time.  
  
• **Abandoned Calls have Positive Impact**: Select this option if you consider a call that is abandoned within the service level threshold time as a treated call. With this configuration, abandoned calls have a positive impact on the service level. |
Enter the time in seconds that calls are to be answered based on your service level agreement, from 0 to 2,147,483,647. The time that you enter in this field is used to report on service level agreements and does not affect how long a call remains in a precision queue. The length of time a call remains in a step is determined by the wait time for each individual step.

<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level Threshold</td>
<td>yes</td>
<td>Enter the time in seconds that calls are to be answered based on your service level agreement, from 0 to 2,147,483,647. The time that you enter in this field is used to report on service level agreements and does not affect how long a call remains in a precision queue. The length of time a call remains in a step is determined by the wait time for each individual step.</td>
</tr>
<tr>
<td>Agent Order</td>
<td>yes</td>
<td>Select an option to determine which agents receive calls from this queue. The ordering of agents does not dictate the agents who are selected into a Precision Queue step. Agents are included or excluded based on the conditions specified for the step. • Longest Available Agent (the default): The default method of agent ordering for a precision queue. The call is delivered to the agent who has been in the available (or ready) state the longest. • Most Skilled Agent: The call is delivered to the agent who has the highest competency sum from all the attributes pertinent to the Precision Queue step. In an agent-rich environment, this can mean that more competent agents would be utilized more than less competent agents. • Least Skilled Agent: The call is delivered to the agent who has the lowest competency sum from all the attributes pertinent to the Precision Queue step.</td>
</tr>
</tbody>
</table>
Select the bucket interval whose bounds are to be used to measure the time slot in which calls are answered.

The field defaults to the system default.

To select a different bucket interval:

1. Click the magnifying glass icon to display Select Bucket Intervals.
2. Click a row to make a selection and close the list.

**Step 3** Click the numbered Step Builder link (Step 1, Step 2, and so on) to build a precision queue step in the Step Builder popup window.

**Step 4** When you have finished adding, click Save.

### Consider If Formula for Precision Queue

If you are not on the last step of the precision queue, then you can enter a Consider If formula for that step. A Consider If formula evaluates a call (within a step) against additional criteria. Each time a call reaches a step with a Consider If expression, the expression is evaluated. If the value for the expression returns as true, the call is considered for the step. If the value returns as false, the call moves to the next step. If no expression is provided for a step, the step is always considered for calls.

To add a Consider If formula, type the formula into the Consider If box. Alternatively, you can use the Script Editor to build the formula and then copy and paste it into the Consider If box. Objects used in Consider If formulas are case-sensitive. All Consider If formulas that you add to a precision queue must be valid. If you add an invalid formula, you cannot save the precision queue. To ensure that the formula is valid, use Script Editor to build and validate the formula.

Only the following scripting objects are valid in a Consider If formula:

- Call
- PQ
- Skillgroup
- ECC
- PQ Step
- Call Type
- Custom Functions (You can create custom functions in Script Editor.)
It is possible that a valid Consider If formula can become invalid. For example, if you delete an object used in the formula after you create or update the precision queue, the formula is no longer valid.

Consider If Formula Examples

- PQ.PQ1.LoggedOn > 1 -- Evaluates whether there is more than one agent logged in to this queue.
- CallType.CallType1.CallsRoutedToday > 100 -- Evaluates whether more than 100 calls of this call type were routed today.
- PQStep.PQ1.1.RouterAgentsLoggedIn > 1 -- Evaluates whether there is more than one router agent logged in to this queue for Step 1.
- CustomFunction(Call.PeripheralVariable1) > 10 -- Evaluates whether this formula using a custom function returns a value greater than 10.

Build Precision Queue Steps

Every precision queue must have a step, and every step must have an Expression. An Expression is a collection of attribute terms.

Procedure

**Step 1**
Click the numbered step link in the Steps panel (Step 1, Step 2, and so on). The step number popup window opens.

**Step 2**
Build the first step as follows.

a) Click the magnifying glass icon to the right of the Select Attribute field in the Expression 1 panel.

b) Select an attribute from the list.

c) Use the two Select fields to establish the terms of the attribute. Click the first Select field to choose an operator.

- For Boolean attributes, choices are the operators for Equal and Not Equal.
- For Proficiency attributes, choices are the operators for True, False, Less Than, Less Than or Equal To, Greater Than, and Greater Than or Equal To.

d) Click the second Select field to choose a value.

- For Boolean attributes, values are True and False.
- For Proficiency attributes, values are numbers from 1 to 10.

Your selection creates an attribute term for the Expression.

**Step 3**
To add a second attribute to the first Expression, click Add Attribute in the Expression 1 row.

a) Select AND or OR to establish the relationship between the first and second attributes.

b) Repeat steps 2b, 2c, and 2d.

**Step 4**
Continue to add attributes to Expression 1.

All attributes within an expression must be joined by the same logical operator. They must all be ANDs, or they must all be ORs.
Step 5  To add a second Expression, click the Add Attribute drop-down in the Expression 1 row and select Add Expression.

Step 6  Select AND or OR to establish the relationship between the first and second Expressions.

Step 7  Add attributes to Expression 2.

Step 8  Continue to add Expressions as needed.

In this example, a Spanish caller located in the Boston area needs an onsite visit from a technician to repair his ServerXYZ. An ideal agent should be fluent in Spanish and have the highest proficiency in ServerXYZ. This can be seen in Expression 1. Expression 2 allows us to specify that the selected agent must also be from either Boston or the New England area.

Step 9  When you have completed the step, click OK to add it to the precision queue.

Step 10  To build the next step, click Add Step. Each successive step is prepopulated with the Expressions and attributes of its predecessor. Decrease the attribute qualifications and competencies in successive steps to lower the bar such that the pool of acceptable agents increases.

Step 11  When you have created all steps, you can open any step except the last and enter values in the Consider if and Wait for fields.

- **Consider if** is a formula that evaluates a call within a step against additional criteria. (See Consider If Formula for Precision Queue, on page 103 for more information about Consider If.)

- **Wait for** is a value in seconds to wait for an available agent. A call will queue at a particular step and wait for an available agent matching that step criteria until the number of seconds specified. A blank wait time indicates that the call will proceed immediately to the next step if no available agents match the step criteria. Wait time defaults to 0 and can take a value up to 2147483647.
Configure routes

The route is a value returned by a routing script that maps to a target or a peripheral. Those targets include services, skill groups, agents, translation routes, queue points, or CTI route points. The Unified CCE converts a route to a device target to direct to the request destination.

When you create a route, you associate the route with a service.

Procedure

**Step 1**  
From the Configuration manager, choose **Tools > Explorer Tools > Skill Group Explorer**. The Skill Group Explorer dialog box opens.

**Step 2**  
Click **Retrieve**.

**Step 3**  
Choose the skill group for which you are creating the route.

**Step 4**  
Click **Add Route**. The Route tab opens.

**Step 5**  
In the Route tab, enter information in the following fields:

- **Skill group priority**. The value 0 indicates a base skill group. This is the default when there is only one skill group and there are no priorities.
- **Name**. The enterprise name of the route.
- **Description**. Enter an optional description of the route.
- **Service Name**: The name for the service.

**Step 6**  
Click **Save**.

---

⚠️ **Caution**  
When you break the association between a route and a peripheral, the Unified CCE removes the Route ID value from all peripheral targets that reference that route.

Perform Bulk Configuration

Access Bulk Configuration Tools

Procedure

**Step 1**  
Double-click **Configuration Manager** in the Administration Data Server group or the Administration Client group.

**Step 2**  
In the Menu selection box, select **Tools > Bulk Configuration**.

**Step 3**  
From the submenu selection list, select **Insert** if you need to insert data or **Edit** if you need to edit.

**Step 4**  
In the next menu selection list, select the type of table with which you need to work.
Add New Records

You can add records by inserting multiple blank rows (records) and filling in the data or by importing the data.

You can also edit the data you insert when you insert it.

Insert New Records

To insert a new record:

Procedure

Step 1 In the Bulk Configuration > Insert menu, select the name of the data table to which you want to add records. The appropriate Insert window opens, automatically displaying one new row.

Step 2 To create additional rows, enter the number of additional rows in the Quantity field and click Insert. The additional rows are added in the Insert window.

Step 3 Enter the data in the rows:

a) If you want to edit individual fields in the new rows, type the information you want in each of the fields and skip to Step 8.

b) If you want to edit a column in multiple rows so that a range of values is entered, continue to Step 4.

Note For other ways of entering data into multiple rows, see Edit Range of Data, on page 110

Step 4 Select the rows in the column you want to modify.

Step 5 Click Edit Range. The Edit Range dialog appears.

Step 6 Enter a prefix (optional), the start value for the range, and a suffix (optional). The generated values are listed in the dialog.

Step 7 Click OK to close the Edit Range dialog and apply the values to the column you selected.

Step 8 When you have finished setting fields in the new rows, press Enter to apply your changes to the Unified CCE database.

Note You can leave empty rows, the system ignores them. No changes are made to the database until you press Enter.

Import Data

You can import data from a specified text file into the opened database table. You can import whole records or only columns of data if the data matches (see Step 3 of the following procedure). The process cancels if any error occurs during the import process.

Procedure

Step 1 In the Insert or Edit window, click Import.

Step 2 In the Import dialog, click File.

Step 3 In the File Open dialog, select the file containing the data that you want to import and click Open. The Import File Data area displays the first few lines of the opened file.

- When importing data in the Edit mode, the following rules apply:
• The Bulk Configuration tool reads only those records whose primary key values match those of records in the Edit window.
  If a record does not match the primary key value, the record is considered to be an error and a message box with the primary key value pops up to ask you to correct the problem.
• If any field in the import record is null, the corresponding field value in the grid window become blank for an edit cell or uses the default value for a drop-down list cell.
• If any field is missing in the import file, the corresponding field in the Edit window remains unchanged.
• If there is a larger number of records in the file to be imported than the number of rows in the grid, it is considered an error and a message box pops up asking you to correct it.
• If there is a duplicated primary key in the file to be imported, it is considered an error and a message box with the duplicated primary key value pops up asking you to correct it.
• After importing, all records imported (including records marked for deletion in the grid) are marked as "Changed" regardless of whether the value is changed or not.
• After importing, the records display in index order (ordered by logical keys). If you did not sort before importing, the order appears the same after the import.

• When importing data in the Insert mode, the following rules apply:
  • Only a single import is supported and any existing rows are removed from the grid. When you click **Import**, the following message box pops up if there is any record in the grid:
    **All the existing data will be replaced by the data to be imported.**
    If you want to retain the current data on the grid please click the Cancel button then save or export the existing data. Click the OK button to proceed with the importing.
  • After importing, all rows are marked as "New" and the ordering is the same as that in the file imported from.
  • In the Import Insert mode, the tool reads only those records whose primary key values are not presented. If the primary key field is selected for file to be imported, it is considered an error and a message box with the primary key field name pops up asking you to correct the problem.
  • If any field in the import record is null, the corresponding field value in the grid window becomes blank for an edit cell or uses the default value for a drop-down list cell.

  **Note** If headers are included in the imported file, the **Add** and **Remove** buttons are not enabled and you can only import the records as a whole. In that case, skip to Step 6.

**Step 4** If the imported data does not contain headers, in the Available Fields list box, select the names of the fields to import that match the data and click **Add**.

**Step 5** To change the order of the columns, select a column and move it within the list by clicking **Up** or **Down**.

**Step 6** Click **OK**. The data is imported into the data table.

---

**Data File Format**
The import and export files used by the Bulk Configuration tool can optionally include a header that identifies the table and columns in the file. The header is followed by one line for each row of data.

The following rules apply to file headers:

- A line beginning with a number sign (#) is a comment and is ignored.
- Blank lines are also ignored.
- The header content is indicated by a line beginning with two underline characters and the word TABLE or COLUMNS. The following line contains the name of the table or the name of the columns. For example:
  
  __TABLE
  Call_Type __
  COLUMNS

  CallTypeID EnterpriseName Description Deleted CustomerDefinitionID

- All column names must be on a single line and are separated by Tab characters.

The following rules apply to the data in the files:

- One row of table data per line.
- Column values must be in the same order in all rows. If columns are specified in the header, the columns in the data rows must be in the same order.
- Column values are separated by a single Tab character.
- Fields intentionally left blank must be represented by two adjacent Tab characters or a Tab character at the end of a line. On import, the default value is used for such a value.
- String values may include spaces.
- An error occurs on import if a line contains too few or too many values.

**Note**

A simple way to create the import file with a valid format is to use Excel and save the file as Text (Tab delimited) (*.TXT).

### Select Data

You can select whole records for importing, exporting, setting security, deleting, or undeleting. Or, you can select the same field in multiple records for simultaneous editing.

**Select Records**

Click in the left-most numbered field in a row to select that row and highlight it. Click in any other field in a row to select the row but not highlight it.

**Select One Field in Multiple Records**

You can select one edit-control field (when there is no section box in the field) in multiple records in any of the following three ways:

- Click the field where you want to start and, keeping the left mouse button held down, move the cursor to the last field.
• Click the field where you want to start. While holding down the `Shift` key, click the last field.
• Click the field where you want to start. While holding down the `Shift` key, click the down arrow to select.
• Press `Ctrl`, then click on each field you wish to select. This allows you to select a discontinuous group of fields.

**Edit Range of Data**

You can edit a range of data in a table column in three ways:

- Apply a single value to a range of edit-control fields
- Apply a single value to a range of selection-box fields
- Apply a range of values to a range of fields

**Apply a Single Value to a Range of Edit-Control Fields**

An *edit-control field* is one you can edit that does not contain a selection box.

To apply a single value to a range of edit-control fields:

**Procedure**

---

**Step 1** Make your selection: click the field where you want the range to start and, keeping the left mouse button held down, move the cursor to the last field in the range.

**Step 2** Type the new entry that you want to appear in all the fields.

**Step 3** Click `Enter` or `Tab`. This applies the change to all the records in the range and moves the focus to the next data field.

**Apply a Single Value to a Range of Selection-Box Fields**

To apply a single value to a range of selection-box fields:

**Procedure**

---

**Step 1** Select the first field where you want the range to start.

**Step 2** Press the `Shift` key and hold it down for steps 3, 4, and 5.

**Step 3** Click the selection-box down arrow but keep the left mouse button held down and select the fields you want in the range.

**Step 4** Click the last field in the selection to display the selection list. You can also open the selection box by pressing `Alt +` an arrow key.

**Step 5** Click your selection.

**Step 6** Click `Enter` or `Tab` (or any other field). This applies the change to all the records and moves the focus to the next data field.
**Apply a Range of Values to a Range of Fields in a Column**

To apply a range of values to a range of fields in a column:

**Procedure**

**Step 1**  
Select the range of fields in a database column. This enables the **Edit Range** button.  
*Note*  
The **Edit Range** button does not work for selection-box fields.

**Step 2**  
Click **Edit Range**. The Edit Range dialog displays.

---

**Figure 2: Edit Range Dialog Box**

---

**Step 3**  
In the Edit Range From field, enter the first number of the range.

**Step 4**  
In the Prefix and Suffix fields, you can optionally enter substrings to appear before or after each value. The Edit Range dialog lists the generated values.  
*Note*  
When entering a numeric range, you may also enter leading zeros to ensure proper alignment (that is, 001 to 999).

**Step 5**  
Click **OK**. This applies the changes to the fields you selected in the Insert or Edit window.
Configure Cisco Unified Intelligence Center

Acquire License

**Procedure**

**Step 1** To acquire the license file, go to the Cisco Product License Registration website at this URL: https://tools.cisco.com/SWIFT/LicensingUI/Home.

**Step 2** If you do not have a Product Authorization Key (PAK), click the available licenses link.

**Step 3** Scroll to Unified communications and click **Cisco Unified Intelligence Center**.

**Step 4** Enter your MAC Address, accept the agreement, and enter your Registrant Information. The MAC Address appears online at the end of the installation. If you need to find the MAC Address again, follow these steps to obtain it:

1. Sign in to the server node, using the credentials of the System Administration user.
2. Enter this CLI command: show status.

**Step 5** Follow prompts to complete the registration windows. You will receive an email from Cisco that contains your license file as an attachment. The file format is *.lic.

**Step 6** Save the license file in a location where the System Application User can access it.

**Warning** Save a backup copy of this file. You can open a *.lic file to look at it, but do not make any changes to it. Changing the file invalidates the license.

Sign In to Administration Console

Who can sign in to the administration console: The System Application User who is the default Superuser.

To upload the license, you must sign in to the Unified Intelligence Center Administration Console. This is the OAMP interface for Unified Intelligence Center. The first person who signs in to the Administration application must do so using the user ID and password that were defined for the System Application User during the installation. This user is the initial Superuser for Unified Intelligence Center Administration.

**Procedure**

**Step 1** Enter this URL: http://<HOST ADDRESS>/oamp, where HOST ADDRESS is the IP address or hostname of your Controller node.

**Step 2** Enter the System Application User ID and password that you defined during installation.
Upload License

After the license file is uploaded to the publisher node, within a minute, it is automatically replicated to all nodes in the cluster.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Administration application, choose <strong>Cluster Configuration &gt; License Management</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click <strong>Browse</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Navigate to the location where the *.lic file was saved.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Apply License</strong> to load the license.</td>
</tr>
</tbody>
</table>

A message appears indicating that the license file was uploaded successfully and will be distributed to other nodes (if any) in the cluster in approximately one minute.

Note: The databases are polled once a minute for changes. The license replication is not immediate but occurs within a minute.

Configure SQL User Account

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Launch Microsoft SQL Server Management Studio on the Unified CCE Administration Client workstation.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Connect to the Side A Logger using the default credentials.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Navigate to <strong>Security &gt; Logins</strong>, right-click <strong>Logins</strong> and select <strong>New Logins</strong>. You use this login when you configure the data sources for Cisco Unified Intelligence Center reporting.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the General Screen:</td>
</tr>
<tr>
<td>a)</td>
<td>Enter the Login Name.</td>
</tr>
<tr>
<td>b)</td>
<td>Select <strong>SQL Server authentication</strong>.</td>
</tr>
<tr>
<td>c)</td>
<td>Enter and confirm the password.</td>
</tr>
<tr>
<td>d)</td>
<td>Uncheck <strong>Enforce password policy</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Navigate to the User Mapping Screen page and perform the following:</td>
</tr>
<tr>
<td>a)</td>
<td>Check the databases associated with Side A and AWdb.</td>
</tr>
<tr>
<td>b)</td>
<td>If you are configuring a SQL user for Live Data, also check the master database.</td>
</tr>
<tr>
<td>c)</td>
<td>Choose each database and associate it with the db_dataloader and public roles, and click <strong>OK</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Repeat this procedure on the Side B Logger.</td>
</tr>
</tbody>
</table>

Related Topics

Configure Live Data with AW, on page 35
set live-data aw-access, on page 238
Configure Data Sources

To integrate Unified Intelligence Center with Unified CCE, you must configure the following two data sources:

• Unified CCE Historical data source—This data source is added by default to support the Unified CCE stock historical reports and Unified CCE User Integration. Complete the Database Host, Database Name, and the Database User ID and Password fields for this data source and ensure that it is online before Unified CCE User Synchronization can occur.

• Unified CCE Realtime data source—This data source is added by default to support the Unified CCE stock real time reports. Complete the Database Host, Database Name, and the Database User ID and Password fields for this data source.

Depending on your environment, the Unified CCE Historical and Realtime data sources can point to the same machine.

You can execute a CLI command to point each node to a unique IP Address for the Unified CCE Historical or Realtime data source. The command is set cuic-properties host-to-ip. For more information about the CLI, see the Administration Console User Guide for Cisco Unified Intelligence Center at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

To integrate Unified Intelligence Center with Unified CVP, you must add a Unified CVP data source.

A Unified Intelligence Center data source is also installed by default. This data source represents the Unified Intelligence Center database on the node that stores records for reports, dashboards, and users maintained on that node. This data is replicated across all nodes in the cluster. You can edit the description for this data source, but do not change other fields. The Unified Intelligence Center data source for each node is configured by default to point to that member.

Configure Unified CCE Data Sources

Placeholders for two Unified CCE data sources appear by default on the Data Sources page. These are the data sources for the data that populates the stock templates. Before you can run reports or can run Unified CCE User Integration, you must edit the parameters of these data sources to complete the configuration, including Database Host, Database port, Database Name, User ID and Password.

The two data sources—Unified CCE Historical and Unified CCE Realtime—contain the same information, but the Unified CCE Historical data source has a lower load volume and is used to gather data for most of the stock value lists and for Unified CCE User Integration.

Before you can run reports or can run Unified CCE User Integration, you must edit the Unified CCE Historical data source to complete the configuration for the Database Host Address, Database Name, IP Address, User ID, and Password.
Procedure

Step 1 From the Unified Intelligence Center Reporting application, click the Data Sources drawer in the left panel to open the Data Sources page.

Step 2 Select the Unified CCE Historical Data Source.

Step 3 Click Edit to open the Data Source Create/Edit page.

Step 4 Complete the fields for this data source. See the online help for guidance.

Step 5 Test the data source connection. Troubleshoot if necessary.

Step 6 Save the data source.

Step 7 Repeat steps 2 through 6 for the Unified CCE Realtime data source.

Create Data Source for Cisco Unified CVP Report Data

Procedure

Step 1 Log in to the Unified Intelligence Center at https://<hostname of CUIC Publisher>:8444/cuic.

Step 2 Select the Data Sources drawer to open the Data Sources page.

Step 3 Click Create to open an Add DataSource window.

Step 4 Complete fields on this page as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of this data source.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this data source.</td>
</tr>
<tr>
<td>Type</td>
<td>Choose Informix.</td>
</tr>
<tr>
<td>Note</td>
<td>Type is disabled in Edit mode.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Enter the IP address or Domain Name System (DNS) name for the Unified CVP Reporting server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number. Typically, the port is 1526.</td>
</tr>
<tr>
<td>Database Name</td>
<td>Enter the name of the reporting database on the Unified CVP reporting server.</td>
</tr>
</tbody>
</table>
**Field** | **Value**
---|---
**Instance** | Specify the instance name of the desired database. By default, this is `cvp`.

**Timezone** | Choose the correct time zone for the data stored in the database. In locations that change from Standard Time to Daylight Savings Time, this time zone is updated automatically.

**Database User ID** | Enter the user ID of the Reporting User who is configured in the Operations Console to access the Unified CVP reporting database.

(The `cvp_dbuser` account is created automatically during Unified CVP Reporting server installation.)

**Password and Confirm Password** | Enter and confirm the password for the database user.

**Charset** | Choose UTF-8.

**Default Permissions** | View or edit the permissions for this datasource for My Group and for the All Users group.

---

**Step 5**  
Click **Test Connection**.  
If the status is not Online, review the error message to determine the cause and edit the data source accordingly.

**Step 6**  
Click **Save** to close the Add Data Source window.  
The new data source appears on the Data Sources list.

---

**Download Report Bundles**

The following Cisco Unified Intelligence Center report bundles are available as downloads from Cisco.com [http://software.cisco.com/download/type.html?mdfid=282163829&catid=null](http://software.cisco.com/download/type.html?mdfid=282163829&catid=null). Click the **Intelligence Center Reports** link to view all available report bundles:

- Realtime and Historical Transitional templates - Introductory templates designed for new users. These templates are simplified versions of the All Fields templates, and are similar to templates available in other contact center solutions.

- Realtime and Historical All Fields templates - Templates that provide data from all fields in a database. These templates are most useful as a basis for creating custom report templates.

- Live Data templates - Templates that provide up to the moment data for contact center activity.

- Realtime and Historical Outbound templates - Templates for reporting on Outbound Option activity. Import these templates if your deployment includes Outbound Option.
- Realtime and Historical Cisco SocialMiner templates - Templates for reporting on SocialMiner activity. Import these templates if your deployment includes SocialMiner.
- Cisco Unified Intelligence Center Admin Security templates - Templates to report on Cisco Unified Intelligence Server audit trails, permissions, and template ownership.

Additionally, sample custom report templates are available from the Cisco Developer Network (http://developer.cisco.com/web/ccr/documentation).

**Import Report Bundles**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>In Unified Intelligence Center, click <strong>Reports</strong> in the left pane.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Import Report</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>In the <strong>File Name (XML or ZIP file)</strong> field, click <strong>Browse</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Browse to and select the report bundle zip file, and click <strong>Open</strong>. Select a report bundle for the version of software deployed in the contact center.</td>
</tr>
<tr>
<td>5</td>
<td>Select the location where you want to save the file.</td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>Import</strong>.</td>
</tr>
<tr>
<td>7</td>
<td>Choose one:</td>
</tr>
<tr>
<td></td>
<td>- If the report or reports do not yet exist, you must provide the data source. From the <strong>Data Source for Value List</strong> drop-down list, select the data source used. Then click <strong>Import</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You have to select a data source for the value list only if it does not use the same data source as the report definition. For LiveData reports, the Data Source for Report Definition is LiveData Streaming and the Data Source for Value List is UCCE Realtime. For real time reports, the Data Source is UCCE Realtime. For historical reports, the Data Source is UCCE Historical.</td>
</tr>
<tr>
<td></td>
<td>- If the report or reports do exist, a message appears asking you if you want to replace the existing report (which overwrites any report definition changes associated to it). Click <strong>Yes</strong>, <strong>Yes to All</strong>, <strong>No</strong>, or <strong>No to All</strong>.</td>
</tr>
</tbody>
</table>

**Configure Unified Intelligence Center Administration**

Complete the following procedure to configure Unified Intelligence Center Administration.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sign in to the <strong>Cisco Unified Intelligence Center Administration Console</strong> (https://&lt;hostname&gt;:8443/oamp).</td>
</tr>
<tr>
<td>2</td>
<td>Configure the Active Directory tab under <strong>Cluster Configuration &gt; Reporting Configuration</strong>.</td>
</tr>
<tr>
<td></td>
<td>a) For Host Address for the Primary Active Directory Server, enter the IP address of the domain controller.</td>
</tr>
</tbody>
</table>
b) For Port, enter the port number for the domain controller.
c) Complete the Manager Distinguished Name fields that are required for the customer.
d) Enter and confirm the password with which the Manager accesses the domain controller.
e) For User Search Base, specify users and the domain name and any sub-domain names.
f) For Attribute for UserID, select sAMAccountName.
g) Add at least one domain for the UserName Identifier. Do not type the @ sign before the domain name.
h) Set a domain as the default.
i) Click Test Connection.
j) Click Save.

Step 3 Configure syslog for all devices.
   a) Choose Device Management > Log and Trace Settings.
   b) For each host address:
      • Select the associated servers.
      • In the Edit Serviceability Settings screen Syslog Settings pane, configure the Primary and Backup Host. Click Save.

Step 4 Configure SNMP for all devices, if used.
   a) Select Network Management > SNMP.
   b) Navigate to SNMP and for each server add the following:
      • V1/V2c Community Strings.
      • Notification Destination.

---

Configure Cisco Unified Customer Voice Portal

Configure Unified CVP Server

Configure Network Card for Unified CVP

Procedure

Step 1 Choose Start and right-click Network.
Step 2 Select Properties. Then select Change Adapter Settings.
Step 3 Press Alt F from the Network Connections page to display the Advanced menu.
Step 4 From the Advanced menu choose Advanced Settings.
Set up Unified CVP Media Service IIS

To simplify Unified CCE scripting, do not define Cisco Unified CVP Media Server IIS in scripts.
Complete the following procedure on each of the CVP servers in the deployment.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose <strong>Start</strong> &gt; <strong>Programs</strong> &gt; <strong>Administrative Tools</strong> &gt; <strong>Server Manager</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Expand <strong>Roles</strong> in the left panel of the Server Manager window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Expand <strong>Web Server (IIS)</strong> and select <strong>Internet Information Services (IIS) Manager</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the <strong>Hostname</strong> in the Internet Information Services Manager window.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Under <strong>IIS</strong>, right-click <strong>Directory Browsing</strong> and select <strong>Open feature</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Enable</strong> on the Action pane. Right-click <strong>Directory Browsing</strong> and click <strong>Start</strong>.</td>
</tr>
</tbody>
</table>

Set Up FTP Server

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Install the FTP Service on the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>Choose <strong>Start</strong> &gt; <strong>Administrative Tools</strong> &gt; <strong>Server Manager</strong>.</td>
</tr>
<tr>
<td>b)</td>
<td>Expand <strong>Roles</strong> in the left panel of the Server Manager window.</td>
</tr>
<tr>
<td>c)</td>
<td>Right-click <strong>Web Server (IIS)</strong> and click <strong>Add Role Services</strong>.</td>
</tr>
<tr>
<td>d)</td>
<td>Check the <strong>FTP Server</strong> check box and then click <strong>Install</strong>, installation takes a few moments.</td>
</tr>
<tr>
<td>e)</td>
<td>When the installation is complete, click <strong>Close</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Enable the FTP Service on the server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>Choose <strong>Start</strong> &gt; <strong>Administrative Tools</strong> &gt; <strong>Server Manager</strong>.</td>
</tr>
<tr>
<td>b)</td>
<td>Expand <strong>Roles</strong> in the left panel of the Server Manager window.</td>
</tr>
<tr>
<td>c)</td>
<td>Expand <strong>Web Server (IIS)</strong> and then click <strong>Internet Information Services (IIS) Manager</strong>.</td>
</tr>
<tr>
<td>d)</td>
<td>Expand hostname.</td>
</tr>
<tr>
<td>e)</td>
<td>Right-click <strong>Sites</strong> and click <strong>Add FTP Site</strong>.</td>
</tr>
<tr>
<td>f)</td>
<td>Enter a <strong>FTP site name</strong>.</td>
</tr>
<tr>
<td>g)</td>
<td>Enter e:\Inetpub\wwwroot in the <strong>Physical path</strong> of the FTP site name, and click <strong>Next</strong>.</td>
</tr>
<tr>
<td>h)</td>
<td>Enter the IP address of the CVP Server.</td>
</tr>
<tr>
<td>i)</td>
<td>Select <strong>No SSL</strong> in SSL Options and then click <strong>Next</strong>.</td>
</tr>
<tr>
<td>j)</td>
<td>Check the <strong>Anonymous</strong> and <strong>Basic</strong> check boxes.</td>
</tr>
<tr>
<td>k)</td>
<td>Select <strong>All Users</strong> from the Allow Access To drop-down list.</td>
</tr>
<tr>
<td>l)</td>
<td>Check the <strong>Read</strong> and <strong>Write</strong> check boxes, and then click <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Set the Basic Setting for the FTP Server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>a)</td>
<td>Click <strong>Sites</strong> and then click the FTP server that you have created.</td>
</tr>
<tr>
<td>b)</td>
<td>Click <strong>Basic Settings</strong> in the Actions tab and click <strong>Connect as</strong>.</td>
</tr>
</tbody>
</table>
c) Select Application user (pass-through authentication) option and click OK twice.

Configure Unified CVP Reporting Server

Create Reporting Users

Unified CVP reporting users can sign in to Unified Intelligence Center only if they exist in the Administration console as Superusers or if Active Directory (AD) is configured in the Unified Intelligence Center Administration console for their domain:

- Superusers who are added are considered to be IP Multimedia Subsystem (IMS) users.
- Users who are authenticated through Active Directory are considered to be Lightweight Directory Access Protocol (LDAP) users. For more information, see Configure Active Directory Server.

Both IMS users and LDAP users can log in to Unified Intelligence Center reporting and are restricted to the limited Login User role until the Unified Intelligence Center reporting security administrator gives them additional roles and flags them as active users.

Create Superusers

Procedure

Step 1 Log in to the Cisco Unified Intelligence Center Administration Console (http://{hostname}/oamp).
Step 2 Navigate to Admin User Management > Admin User Management to open the Users page.
Step 3 Click Add New to add and configure a new user or click an existing username to edit the configuration for that user.
This page has three tabs: General, Credentials, and Policy. For information about completing these tabs, see Administration Console User Guide for Cisco Unified Intelligence Center at http://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html or the Administration console online help.
Step 4 Click Save.

Set Up Active Directory Server for LDAP Users

Configure the Active Directory tab in the Cisco Unified Intelligence Center Administration console so that Unified CVP reporting users can log in to the Unified Intelligence Center reporting application with the user name and password that is defined in their domain.
**Procedure**

**Step 1** In the Cisco Unified Intelligence Center Administration application, navigate to **Cluster Configuration** > **Reporting Configuration** and select the Active Directory tab.

**Step 2** Complete all fields on this page, referring to the online help for guidance.

**Step 3** Click **Test Connection**.

**Step 4** When the connection is confirmed, click **Save**.

**Sign In to Cisco Unified Intelligence Center Reporting Interface**

Who can sign into the Unified Intelligence Center reporting interface:

- Initially, the System Application User who is the default Superuser.
- Eventually, any Unified CVP user who was created in the Administration Console as an IMS superuser or an LDAP user.

**Procedure**

**Step 1** Sign into the Cisco Unified Intelligence Center Administration Console (**http://{hostname}/oamp**).

**Step 2** Navigate to **Control Center > Device Control**.

**Step 3** Click on the name of the Member node you want to access. This opens the Cisco Unified Intelligence Center login page for that member.

**Step 4** Enter your user ID and password. The Overview page appears.

**Create Data Source and Import Report Templates**

**Obtain Cisco Unified CVP Report Templates**

Who can obtain import Unified CVP report templates: any user in your organization.

The Unified CVP reporting template XML files are installed with Unified CVP. Locate them and copy them to a Cisco Unified Intelligence Center client workstation.

**Procedure**

**Step 1** In the Unified CVP server, locate the Unified CVP template files. These are XML files that reside on the reporting server in `%CVP_HOME%\CVP_Reporting_Templates`. You can also find them in the Installation directory `\Downloads and Samples\Reporting Templates`.

**Step 2** Choose the files and copy them to the client computer from where you can launch the Unified Intelligence Center Reporting web application.
Import Unified CVP Report Templates and Set Data Source

Procedure

Step 1 Launch the Unified Intelligence Center web application using the URL http://<HOST ADDRESS>:8444/cuic.
Step 2 Enter your User Name and Password.
Step 3 Click Reports.
Step 4 Right-click the top Reports folder and select Create Sub-Category.
Step 5 Name the new sub-category as a container for Unified CVP reports. Click OK.
Step 6 Click Import Reports.
Step 7 Browse to the location where you copied the Unified CVP Reporting templates files.
Step 8 Click Import.
Step 9 Save to the Unified CVP sub-category folder you created in Step 5.
Step 10 Click Import.
Step 11 Repeat for the callback templates.

Configure Unified CVP Operations Console

Enable Unified CVP Operations Console

Complete the following procedure on the Unified CVP OAMP server to enable the Unified CVP Operations Console.

Procedure

Step 1 Go to Start > Run and type services.msc.
Step 2 Check that Cisco CVP OPSCConsoleServer service is running. If it is not, right-click that service and click Start.
Step 3 Go to Start > All Programs > Cisco Unified Customer Voice Portal > Operation Console to open the Unified CVP OPSCConsole page. If you are using Microsoft Internet Explorer, you will need to accept the self-signed certificate.
Configure Unified CVP Call Server Component

Procedure

Step 1 On the Unified CVP OAMP server, go to Start > All Programs > Cisco Unified Customer Voice Portal.
Step 2 Click Operations Console and log in.
Step 3 Navigate to Device Management > Unified CVP Call Server.
Step 4 Click Add New.
Step 5 On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server. Check ICM, IVR, and SIP. Click Next.
Step 6 Click the ICM tab. For each of the Cisco Unified CVP Call Servers, retain the default port of 5000 for the VRU Connection Port.
Step 7 Click the SIP tab:
   a) In the Enable outbound proxy field, select No.
   b) In the Use DNS SRV type query field, select Yes.
   c) Check Resolve SRV records locally.
Step 8 Click the Device Pool tab. Make sure the default device pool is selected.
Step 9 (Optional) Click the Infrastructure tab. In the Configuration Syslog Settings pane, configure these fields as follows:
   a) Enter the IP address or the hostname of the syslog server.

Example:
Prime server
b) Enter 514 for the port number of the syslog server.
c) Enter the name of the backup server to which the reporting server writes log messages.
d) In the Backup server port number field, enter the port number of the backup syslog server.
Step 10 Click Save & Deploy.
Step 11 Repeat this procedure for the remaining Unified CVP Call Servers.

Configure Unified CVP VXML Server Component

Procedure

Step 1 In the Unified CVP Operations console, navigate to Device Management > Unified CVP VXML Server.
Step 2 Click Add New.
Step 3 On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server.
Step 4 Configure the primary and backup CVP Call Servers as follows:
   a) For CVP-1A, the primary call server is CVP-1A and the backup call server is CVP-1B.
   b) For CVP-2A, the primary call server is CVP-2A and the backup call server is CVP-2B.
   c) For CVP-1B, the primary call server is CVP-1B and the backup call server is CVP-1A.
Configure Unified CVP Media Server

Procedure

Step 1 In the CVP Operations Console, navigate to Device Management > Media Server.
Step 2 Click Add New.
Step 3 On the General tab, configure the following.
   a) Enter the IP address and the hostname of the Unified CVP server.
   b) Check FTP Enabled.
   c) Either Check Anonymous Access or enter the credentials.
   d) Click Test Sign In to validate the FTP access.
Step 4 Click Save.
Step 5 Repeat Steps 1 through 4 for all CVP Servers.
Step 6 In the CVP Operations Console, navigate to Device Management > Media Server.
Step 7 Change Default Media Server from None to any one of the Unified CVP servers. Then click Set.
Step 8 Click Deploy.

Install Unified CVP licenses

Procedure

Step 1 Sign in to the CVP Operations Console.
Step 2 Choose Bulk Administration > File Transfer > Licenses.
Step 3 In the Select device type field, choose All Unified CVP devices.
Step 4 Browse and select the license file.
Step 5 Click Transfer.
Step 6 Click File Transfer Status to monitor transfer progress.
Configure Gateways

If you are using Internet Explorer 11, you must add the Unified CVP Operations Console URL to Internet Explorer's list of Compatibility View websites in order to use the Operations Console. Compatibility View settings are available from Internet Explorer's Tool menu.

Procedure

**Step 1** In the Unified CVP Operations Console, navigate to **Device Management > Gateway**.
**Step 2** Click **Add New**.
**Step 3** On the General tab, configure as follows:
- a) Enter the IP address.
- b) Enter the hostname.
- c) Choose the Device Type.
- d) In the Username and Passwords pane, enter the username, password, and enable password.
**Step 4** Click **Test Sign-in** to verify that a connection with the gateway can be established and that the credentials are correct.
**Step 5** Click **Save**.
**Step 6** Repeat for every gateway.

Add Unified CCE Devices

Procedure

**Step 1** Log in to the **Unified CVP Operations Console**.
**Step 2** Choose **Device Management > Unified ICM**.
**Step 3** Click **Add New**.
**Step 4** On the General tab, configure as follows:
- a) Enter the IP address.
- b) Enter the Hostname.
- c) Check Enable Serviceability.
- d) Enter the Username.
- e) Enter the Password.
- f) Confirm Password.
- g) Accept the default port.
**Step 5** Click **Save**.
**Step 6** Repeat Steps 1 to 5 for all Unified CCE machines.
Add Unified Communications Manager Devices

**Procedure**

**Step 1** Log in to the CVP Operations Console.

**Step 2** Choose Device Management > Unified CM.

**Step 3** Click Add New.

**Step 4** On the General tab, configure as follows:
   a) Enter the IP address.
   b) Enter the Hostname.
   c) Check Enable Synchronization.
   d) Enter the Username.
   e) Enter the Password.
   f) Confirm Password.
   g) Accept the default port.

**Step 5** Click Save.

**Step 6** Repeat Steps 1 to 5 for all Unified Communications Manager Devices.

---

Add Unified Intelligence Center Devices

**Procedure**

**Step 1** Log in to the CVP Operations Console.

**Step 2** Navigate to the Cisco Unified Intelligence Center Device. Choose Device Management > Unified IC.

**Step 3** Click Add New.

**Step 4** On the General tab, configure as follows:
   a) Enter the IP address.
   b) Enter the Hostname.
   c) Check Enable Serviceability.
   d) Enter the Username.
   e) Enter the Password.
   f) Confirm Password.
   g) Accept the default port.
   h) Associate all the existing CVP Reporting Servers.

**Step 5** Click Save.
Transfer Scripts and Media Files

Create the notification destination and deploy to all of the Unified CVP devices.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Unified CVP Operations Console, navigate to <strong>Bulk Administration &gt; File Transfer &gt; Scripts &amp; Media</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Select device type field, select the <strong>Gateway</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Move all Gateways to <strong>Selected</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Default Gateway files</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Transfer</strong> and select <strong>OK</strong> at the popup window.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>File Transfer Status</strong> to monitor transfer progress.</td>
</tr>
</tbody>
</table>

Configure SNMP


**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Unified CVP Operations Console, navigate to <strong>SNMP &gt; V1/V2c &gt; Community String</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click <strong>Add New</strong>.</td>
</tr>
<tr>
<td></td>
<td>a) Name the community string.</td>
</tr>
<tr>
<td></td>
<td>b) Select the <strong>Devices</strong> tab and assign the SNMP community string to a device.</td>
</tr>
<tr>
<td></td>
<td>c) Click <strong>Save and Deploy</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create the notification destination and deploy to all of the Unified CVP devices.</td>
</tr>
<tr>
<td></td>
<td>a) Navigate to <strong>SNMP &gt; V1/V2c &gt; Notification Destination</strong>.</td>
</tr>
<tr>
<td></td>
<td>b) Complete the fields.</td>
</tr>
<tr>
<td></td>
<td>c) Select the <strong>Devices</strong> tab and assign the SNMP notification destination to a device.</td>
</tr>
<tr>
<td></td>
<td>d) Click <strong>Save and Deploy</strong>.</td>
</tr>
</tbody>
</table>

Configure SIP Server Group

SIP Server Groups are required for Cisco Unified Communications Manager and Gateways.
Procedure

Step 1  In the Unified CVP Operations Console, navigate to System > SIP Server Group.

Step 2  Create a server group for the Cisco Unified Communications Manager devices:
   a) On the General tab, click Add New.
   b) Fill in the SRV Domain Name FQDN field with a value that will also be used in the Cluster FQDN setting in Enterprise Parameters in Communications Manager. For example, cucm.cisco.com.
   c) In the IP Address/Hostname field, enter an IP address or hostname for the Unified Communications Manager node.
   d) Click Add.
   The FQDN should match the FQDN configured in the Enterprise Cluster FQDN setting on the Cisco Unified Communications Manager. For example, cucm.cisco.com. Adding the cluster subscriber nodes will load balance across all sub nodes.

Step 3  Create a server group for the gateway devices:
   a) On the General tab, click Add New.
   b) In the SRV Domain Name FQDN field, enter the SRV Domain Name FQDN. For example vxmlgw.cisco.com.
   c) In the IP Address/Hostname field, enter an IP address or hostname for each gateway.
   d) Click Add.
   e) Repeat Steps c and d for each gateway. Click Save.
   Add all VXML gateways as appropriate for deployment and branches. Adding all VXML gateways to the server group will load balance calls across all the member server group gateways.

Step 4  Associate these server groups to all Unified CVP Call Servers:
   a) On the Call Server Deployment tab, move all Unified CVP Call Servers from the Available list to the Selected list.
   b) Click Save and Deploy.

Configure Dialed Number Patterns

Dialed number patterns are required for:
   • Agent Device
   • Network VRU
   • Ringtone
   • Error

Procedure

Step 1  In the Unified CVP Operations Console, navigate to System > Dialed Number Pattern.

Step 2  For each dialed number pattern in the table below:
a) Click **Add New**.
b) In the **Dialed Number Pattern** field, enter the dialed number pattern.
c) In the **Description** field, enter a description for the dialed number pattern.
d) In the **Dialed Number Pattern Types** pane, check the specified dialed number pattern types.
e) Click **Save**.

**Step 3**
After you configure all dialed number patterns, click **Deploy**.

**Step 4**
Click **Deployment Status** to make sure that you applied the configuration.

<table>
<thead>
<tr>
<th>Dialed number pattern</th>
<th>Description</th>
<th>Dialed number pattern types</th>
</tr>
</thead>
<tbody>
<tr>
<td>91*</td>
<td>Ringtone</td>
<td>Check <strong>Enable Local Static Route</strong>. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com). Check <strong>Enable Send Calls to Originator</strong>.</td>
</tr>
<tr>
<td>92*</td>
<td>Error</td>
<td>Check <strong>Enable Local Static Route</strong>. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com). Check <strong>Enable Send Calls to Originator</strong>.</td>
</tr>
<tr>
<td>The agent extension pattern. For example, enter 500* where the range of agent extensions is 5001 to 500999.</td>
<td>Agent Device. Not applicable to SCC Deployment model.</td>
<td>Check <strong>Enable Local Static Route</strong>. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both the Unified Communications Manager gateway. Check <strong>Enable RNA Timeout for Outbound Calls</strong>. The timeout is 60 seconds.</td>
</tr>
<tr>
<td>777*</td>
<td>Network VRU Label</td>
<td>Check <strong>Enable Local Static Route</strong>. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example vxmlgw.cisco.com). Check <strong>Enable Send Calls to Originator</strong>.</td>
</tr>
</tbody>
</table>

**Step 5**
Restart the Unified CVP Call Server components.
Configure Cisco Unified Communications Manager

Set Up Device Pool

Complete the following procedure to configure a device pool.

Procedure

- **Step 1** Choose System > device pool.
- **Step 2** Click Add new.
- **Step 3** Provide an appropriate device pool name in **Device Pool Name**.
- **Step 4** Select a corresponding Call manager group in **Cisco Unified Communications Manager group**.
- **Step 5** Select an appropriate Media resource group list in **Media Resource Group List**.
- **Step 6** Click Save.

Set Up Unified Communications Manager Groups

Complete the following procedure to add a Unified Communications Manager to the Unified Communications Manager Group.

Before you configure a Unified Communications Manager Group, you must configure the Unified Communications Managers that you want to assign as members to that group.

Procedure

- **Step 1** Login to the **Cisco Unified Communication Manager Administration** page, choose System > Server.
- **Step 2** Make sure that you configured both the Publisher and Subscriber.
- **Step 3** Choose System > Cisco Unified CM.
- **Step 4** Click Find.
- **Step 5** Make sure that you configured both the Publisher and Subscriber.
- **Step 6** Choose System > Cisco Unified CM Group.
- **Step 7** Add both Cisco Unified Communications Managers to the Default Unified Communications Manager Group.
- **Step 8** Click Save.

Set Up CTI Route Point

Complete the following procedure to add a computer telephony integration (CTI) route point for agents to use for transfer and conference.
Procedure

Step 1  Choose Device > CTI Route Point.
Step 2  Click Add New.
Step 3  Use the wildcard string XXXX to represent the digits of the dialed number configured on the Unified CCE.
Note   For example, the preconfigured dialed number in the Unified CCE for an agent phone is 10112.
Step 4  Click Save.

Set Up Trunk

Complete the following procedure to configure a trunk for the Unified CVP Servers.

Procedure

Step 1  Choose Device > Trunk.
Step 2  Click Add New.
Step 3  From the Trunk Type drop-down list, choose SIP Trunk, and then click Next.
Step 4  In the Device Name field, enter a name for the SIP trunk.
Step 5  In the Description field, enter a description for the SIP trunk.
Step 6  Click Next.
Step 7  In the Trunk Configuration window, enter the appropriate settings:
   a) Do not check the Media Termination Point Required check box.
   b) From the DTMF Signaling Method drop-down list, choose RFC 2833.
   c) From the SIP Profile drop-down list, choose Standard SIP Profile.
Step 8  Click Save.

Set Up Application User

Procedure

Step 1  Choose User Management > Application User.
Step 2  In the Application User Configuration window, click Add New.
Step 3  Enter the UserID that you entered in Set Up Enterprise Parameters, on page 135. Unified CCE defines the user ID as pguser.
Step 4  Enter cisco in the Password field.
Note   If you change this user ID or password in Unified CCE, you must also change the Unified Communications Manager application user configuration.
**Step 5**  Add the application user to the Standard CTI Enabled Group and Role:
   a) Click *Add to Access Control Group*.
   b) Select the *Standard CTI Enabled* group.
   c) Select the *Standard CTI Allow Control of Phones supporting Connected Xfer and conf* group.
   d) Select the *Standard CTI Allow Control of Phones supporting Rollover Mode* group.
   e) Click *Add Selected*.
   f) Click *Save*.

**Step 6**  Associate the CTI route points and the phones with the application user.

**Step 7**  Click *Save*.

---

**Set Up SIP Options**

**Procedure**

**Step 1**  Choose *Device > Device Settings > SIP Profile*.

**Step 2**  Find and select *Standard SIP Profile*.

**Step 3**  Check *Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"*.

**Step 4**  Click *Save*.

**Step 5**  Click *Reset*.

---

**Set Up Route Pattern**

**Procedure**

**Step 1**  Choose *Call Routing > Route Hunt > Route Pattern*.

**Step 2**  Add a route pattern for the A-side Unified CVP routing clients.
   a) Click *Add New*.
   b) In the Route Pattern field, enter 999911!
   c) In the Gateway/Route List field, choose *SIPTRK_to_CVP_1*.
   d) Click *Save*.

**Step 3**  Add a route pattern for the B-side Unified CVP routing clients.
   a) Click *Add New*.
   b) In the Route Pattern field, enter 999922!
   c) In the Gateway/Route List field, choose *SIPTRK_to_CVP_2*.
   d) Click *Save*.

**Step 4**  Add a route pattern for the Cisco Unified Communications Manager routing client.
a) Click Add New.
b) In the Route Pattern field, enter 999933!
c) In the Gateway/Route List field, choose SIPTRK_to_CVP_1.
d) Click Save.

Note  These route patterns must match the network VRU label defined in Unified CCE. The predefined network VRU label for the side A is 999911010. The predefined network VRU label for the side B is 9999221010. The predefined network VRU label for Unified Communications Manager is 9999331010.

Set Up Conference Bridge

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Media Resources &gt; Conference bridge.</td>
</tr>
<tr>
<td>2</td>
<td>Add a conference bridge for each ingress/VXML combination gateway in the deployment.</td>
</tr>
<tr>
<td>3</td>
<td>In the Conference Bridge name field, enter a unique identifier for the conference bridge name that coincides with the configuration on the gateway.</td>
</tr>
<tr>
<td>4</td>
<td>Click Save.</td>
</tr>
<tr>
<td>5</td>
<td>Click Apply Config.</td>
</tr>
</tbody>
</table>

Set Up Media Termination Point

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Media Resources &gt; Media Termination Point.</td>
</tr>
<tr>
<td>2</td>
<td>Add a media termination point for each ingress/VXML combo gateway in the deployment.</td>
</tr>
<tr>
<td>3</td>
<td>In the Media Termination Point Name field, enter a media termination point name for each ingress/VXML combo gateway in the deployment.</td>
</tr>
<tr>
<td>4</td>
<td>Click Save.</td>
</tr>
<tr>
<td>5</td>
<td>Click Apply Config.</td>
</tr>
</tbody>
</table>
Set Up Transcoder

Procedure

Step 1  Choose Media Resources > Transcoder.
Step 2  Add a transcoder for each ingress/VXML combo gateway in the deployment.
Step 3  In the Device Name field, enter a unique identifier for the transcoder that coincides with the configuration on the gateway.
Step 4  Click Save.
Step 5  Click Apply Config.

Set Up Media Resource Group

Complete the following procedure to configure a media resource group for conference bridge, media termination point, and transcoder.

Procedure

Step 1  Choose Media Resources > Media Resource Group.
Step 2  Add a Media Resource Group for Conference Bridges.
Step 3  Select all the hardware conference bridge resources configured for each ingress/VXML combination gateway in the deployment and add them to the group.
Step 4  Click Save.
Step 5  Choose Media Resources > Media Resource Group.
Step 6  Add a Media Resource Group for Media Termination Point.
Step 7  Select all the hardware media termination points configured for each ingress/VXML combination gateway in the deployment and add them to the group.
Step 8  Click Save.
Step 9  Choose Media Resources > Media Resource Group.
Step 10 Add a Media Resource Group for Transcoder.
Step 11 Select all the transcoders configured for each ingress/VXML combination gateway in the deployment and add them to the group.
Step 12 Click Save.

Set Up and Associate Media Resource Group List

Complete the following procedure to configure and associate a media resource group list. Add the media resource group list to the following devices and device pool.
Procedure

Step 1  Choose Media Resources > Media Resource Group List.
Step 2  Add a Media Resource Group list and associate all of the media resource groups.
Step 3  Click Save.
Step 4  Choose System > Device Pool.
Step 5  Click Default.
Step 6  From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.
Step 7  Click Save.
Step 8  Click Reset.
Step 9  Choose Device > CTI Route Point.
Step 10 Click the configured CTI Route Point. For more information, see Set Up CTI Route Point, on page 130.
Step 11 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.
Step 12 Click Save.
Step 13 Click Reset.
Step 14 Choose Device > SIP Trunk.
Step 15 Click the configured SIP Trunk for side A. For more information, see Set Up Trunk, on page 131.
Step 16 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.
Step 17 Click Save.
Step 18 Click Reset.
Step 19 Click the configured SIP Trunk for side B. For more information, see Set Up Trunk, on page 131.
Step 20 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.
Step 21 Click Save.
Step 22 Click Reset.

Set Up Enterprise Parameters

Procedure

Step 1  Choose System > Enterprise Parameter.
Step 2  Configure the Cluster Fully Qualified Domain Name, ccm.hcscc.icm.

Note  The Cluster Fully Qualified Domain Name is the name of the Unified Communications Manager Server Group defined in Unified CVP.

Configure Mobile Agent

Complete the following procedure to configure CTI ports for Unified Mobile Agent.
## Procedure

1. **Step 1** In Unified Communications Manager Administration, choose **Device > Phone**.
2. **Step 2** Click **Add a New Phone**.
3. **Step 3** Select **CTI Port** from the **Phone Type** drop-down list.
4. **Step 4** Click **Next**.
5. **Step 5** In **Device Name**, enter a unique name for the local CTI Port pool name; click **OK** when finished. Using the example naming convention format LCPxxxxFyyyy:
   a) LCP identifies the CTI Port as a local device.
   b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
   c) yyyy is the local CTI Port.
      The name LCP5000F0000 would represent CTI Port: 0 in a local CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.
6. **Step 6** In Description, enter text identifying the local CTI Port pool.
7. **Step 7** Use the **Device Pool** drop-down list to choose the device pool to which you want network CTI Port pool assigned. (The device pool defines sets of common characteristics for devices.)
8. **Step 8** Click **Save**.
9. **Step 9** Highlight a record and select **Add a New DN**.
10. **Step 10** Add a unique directory number for the CTI port you just created.
11. **Step 11** When finished, click **Save and Close**.
12. **Step 12** Repeat the above steps to configure the network CTI Port pool.
13. **Step 13** In **Device Name**, enter a unique name for the local CTI Port pool name; click **OK** when finished. Using the example naming convention format RCPxxxxFyyyy, where:
   a) RCP identifies the CTI Port as a network device.
   b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
   c) yyyy is the network CTI Port.
      The name RCP5000F0000 would represent CTI Port: 0 in a network CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.
14. **Step 14** In Description, enter text identifying the network CTI Port pool.
15. **Step 15** Use the **Device Pool** drop-down list to choose the device pool to which you want network CTI Port pool assigned. (The device pool defines sets of common characteristics for devices.)
16. **Step 16** Click **Save**.
17. **Step 17** Highlight a record and select **Add a New DN**.
18. **Step 18** Add a unique directory number for the CTI port you just created.
19. **Step 19** When finished, click **Save and Close**.

## Configure Local Trunk

Complete the following procedure to configure Unified Communications Manager for Local Trunk.
**Procedure**

**Step 1**  
From Unified Communications Manager Administration choose System > Location.

**Step 2**  
Click Find to list the locations and add new ones with appropriate bandwidth (8000).

**Step 3**  
For the branch phones, configure each phone so that it is assigned the branch location for that phone.
   a) Choose Device > Phone.
   b) Click Find to list the phones.
   c) Select a phone and set the Location field.

**Step 4**  
Verify that the Cisco AXL Web Service is started and that an Application User is defined and has a role of Standard AXL API Access.
   a) Select Cisco Unified Serviceability from the Navigation drop-down list and click Go.
   b) Navigate to Tools > Control Center > Feature Services.
   c) Start the Cisco AXL Web Service, if it is not started.
   d) From Unified Communications Manager Administration, choose User Management > Application User. Verify you have a user with the role of Standard AXL API Access, or create a new one and add that user to a group that has the role of Standard AXL API Access.

**Deploy SIP Trunk**

Complete the following procedure to deploy the SIP trunk for local trunk:

**Procedure**

**Step 1**  
Using Unified Communications Manager, create a SIP trunk toward the SIP proxy server and select the Phantom location.

**Step 2**  
Create a SIP trunk for each ingress gateway and make the location of these ingress TDM-IP gateways the actual branch location.

**Step 3**  
Create a route pattern pointing the Network VRU Label of the Unified Communications Manager routing client to the SIP trunk toward the SIP proxy. The SIP proxy should route the Network VRU label of the Unified Communications Manager routing client to the Unified CVP Servers.

**Step 4**  
For any IP-originated calls, associate the Unified Communications Manager route pattern with the SIP trunk.

**Step 5**  
Using the Unified Communications Manager Administration, choose Device > Device Settings > SIP Profile > Trunk Specific Configuration > Reroute Incoming Request to new Trunk based on > Call-Info header with the purpose equal to x-cisco-origIP.

**Step 6**  
Associate the new SIP profile with the SIP trunk and each ingress gateway.

**Configure Outbound Dialer**

Complete the following procedure to configure Unified Communications Manager:
Procedure

**Step 1** Log in to the Unified Communications Manager administration page.

**Step 2** Select Devices > Trunk.

**Step 3** Create a SIP trunk to Outbound gateway.

---

**Configure A-Law Codec**

Complete the following procedure to configure Unified Communications Manager.

Procedure

**Step 1** Click the System.

**Step 2** Select Service Parameters.

**Step 3** Select a Server.

**Step 4** Select the service as Cisco Call Manager(Active).

**Step 5** Under Clusterwide Parameters (system-location and region), ensure the following:

- G.711 A-law Codec Enabled is Enabled.
- G7.11 mu-law Codec Enabled to Disabled.

**Step 6** Click Save.

---

**Configure Support for Multiline Agent Control**

To enable reporting and control of secondary lines—particularly in deployments that have agents using phones that require Join Across Line to be enabled—you must follow these configuration steps on Unified Communications Manager.

Multiline Agent Control supports a maximum of four lines per phone, one ACD line and up to three non-ACD lines.

Shared lines are not supported for ACD or non-ACD lines; you cannot have two or more agents that share a common extension on their phones.

Procedure

**Step 1** Enable the Application User for the agent peripheral with the role of Standard CTI Allow Control of Phones supporting Connected Xfer and conf to support phones that require Join Across Line setting on the hard phone.

**Step 2** Configure all agent phones with the following parameters:
Configure RSM

Configure the Cisco Remote Silent Monitoring (RSM) Server in distributed mode, through Cisco Unified Communications Manager.

To facilitate the configuration of RSM, you can use the Unified Communications Manager Bulk Administration Tool (BAT) to automatically create and add line DNs to your simphone devices. Consider this approach if the number of simphones you need to create is large.

Related Topics

Use Simphone Bulk Administration Tool, on page 142

Configure Simulated Phone

You must determine how many simulated phones (also called as simphones) to assign to each Unified Communications Manager cluster. Each cluster must have a number of simphones greater than or equal to the maximum number of agents that will be simultaneously monitored through RSM for the cluster. This section provides the following information:

• To configure the simphone device dependencies, to create a Unified Communications Manager group, RSM region, device pool, route partition, and calling search space.
• To create the simphone devices and assign MAC addresses.
• To add line DNs to the simphone devices.

The procedures describe how to create one simphone and its associated line DN. Additional simphones can be created by using Unified Communications Manager's super copy feature or by creating a batch file.

Note

You must be logged in to the Administration interface of a Unified Communications Manager cluster before you can configure your simphones as described below.

Create Simphone Device Dependencies

Procedure

Step 1

To create a Unified Communications Manager group:

a) Navigate to System > Cisco Unified CM Groups.
b) Click Add New.
c) Enter RSMSimPhone for the Unified Communications Manager group name.
d) Assign the necessary Unified Communications Managers to the group. If you have more than one Unified Communications Manager in the cluster, select the subscribers to be part of the group but do not select the publisher.

e) Click **Save**.

**Step 2**  
To create a simphone region:

a) Navigate to System > Region Information > Region.

b) Click **Add New**.

c) Enter **RSMSimPhone** for the region name, adding prefix or suffix naming conventions, if required.

d) Click **Save**.

e) Add relationships with agent phones to the regions in your environment. Note that calls between simphones and agent phones must use the G.729 codec.

f) Click **Save**.

**Step 3**  
To create a simphone device pool:

a) Navigate to System > Device Pool.

b) Click **Add New**.

c) Enter **RSMSimPhone** for the device pool name, adding prefix or suffix naming conventions, if required.

d) Select the **RSMSimPhone** Communications Manager group from the Device Pool Settings > Cisco Unified Communications Manager Group drop-down list.

e) Select **RSMSimPhone** region from the Roaming Sensitive Settings > Region drop-down list.

f) Enter the remaining parameters, according to your configuration (for example, date/time group and user locale.)

g) Click **Save**.

**Step 4**  
To create a Device Feature Group

a) Choose General Administration > Feature Groups.

b) Select the customer instance. For example, Customer_1.

c) Click **Add** and enter the following values:

1. Name - **CC-RSM**.

2. Description - **Contact Center RSM Group**.

3. Outbound calls limitations - **National24Hrs-Standard-wCC**.

4. Call forward limitations - **Default CoS**.

5. Voicemail Template - **Basic voicemail service type**.

6. Inbound call options - **Allow two Direct Dial Inward lines**.

7. Number of extensions or lines - **Two Numbers: DDI or Extension**.

8. Idle URL: None.

d) Under the Value Add panel, select features as required.

e) Under Common Line Settings (Line Feature) panel, check the Contact Center Agent Line feature.

f) Under Private line settings (phone line feature) panel, check **Recording Option**, **Recording Profile**, **Call waiting busy trigger**, **Max calls waiting**

g) Under Handset panel check **Built-in Bridge** check-box.

h) Click **Submit**.

**Step 5**  
To create a simphone route partition:

a) Navigate to Call Routing > Class of Control > Partition.

b) Click **Add New**.
c) Enter **RSMSimPhone** in the text box, adding prefix or suffix naming conventions, if required.
d) Click **Save**.

**Step 6**  
To create a simphone calling search space:
a) Navigate to **Call Routing > Class of Control > Calling Search Space**.
b) Click **Add New**.
c) Enter **RSMSimPhone** for the calling search space name, adding prefix or suffix naming conventions, if required.
d) Select the route partition containing the agent phones that RSM will monitor from the Available Partitions selection box, and move them to the Selected Partitions selection box.
e) Click **Save**.

**Note**  
For 4000 agent deployment, repeat this procedure for the second PG.

---

**Create Simphone Device**

**Procedure**

**Step 1**  
Navigate to **Device > Phone**.

**Step 2**  
Click **Add New** to create a new phone device.

**Step 3**  
Select **Cisco 7941** for the phone type, then click **Next**.

**Step 4**  
Choose **SIP** for the device protocol, then click Next. The Phone Configuration page appears.

**Step 5**  
Enter the MAC address.

**Step 6**  
Enter the parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Pool</td>
<td>RSMSimPhone</td>
</tr>
<tr>
<td>Phone Button Template</td>
<td>Standard 7941 SIP</td>
</tr>
<tr>
<td>Location</td>
<td>Relevant environment</td>
</tr>
<tr>
<td>Built In Bridge</td>
<td>Off</td>
</tr>
<tr>
<td>Phone Personalization</td>
<td>Disabled</td>
</tr>
<tr>
<td>Allow Device Control through CTI</td>
<td>Yes</td>
</tr>
<tr>
<td>Presence Group</td>
<td>Standard</td>
</tr>
<tr>
<td>Device Security Profile</td>
<td>Cisco 7941 Standard Non-Secure SIP</td>
</tr>
<tr>
<td>SIP Profile</td>
<td>Standard</td>
</tr>
<tr>
<td>Maximum Calls</td>
<td>2 (two)</td>
</tr>
<tr>
<td>Busy Trigger</td>
<td>1 (one)</td>
</tr>
</tbody>
</table>

**Step 7**  
Click **Save**.
The simphone device is created.

**Note** Parameters not listed can be left to their default settings.

---

**Associate a Line DN to Simphone Device**

**Procedure**

**Step 1** Click the **Line [1] - Add a new DN** link in the Association Information panel.

**Step 2** Enter the parameters. Parameters that are marked with an asterisk (*) are optional; those not listed may be left to their default settings.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Number</td>
<td>5040</td>
</tr>
<tr>
<td>Route Partition</td>
<td>RSMSimPhone</td>
</tr>
<tr>
<td>CTI Control</td>
<td>Yes</td>
</tr>
<tr>
<td>Voice Mail Profile</td>
<td>No voicemail</td>
</tr>
<tr>
<td>Calling Search Space</td>
<td>RSMSimPhone</td>
</tr>
<tr>
<td>Presence Group</td>
<td>Standard Presence group</td>
</tr>
<tr>
<td>User Hold MOH Audio Source</td>
<td>1-SampleAudioSource</td>
</tr>
<tr>
<td>Network Hold MOH Audio Source</td>
<td>1-SampleAudioSource</td>
</tr>
<tr>
<td>Line1 on Device &lt;MAC ADDR&gt;</td>
<td>RSM SimPhone</td>
</tr>
<tr>
<td>Monitoring Calling Search Space (CSS)</td>
<td></td>
</tr>
</tbody>
</table>

**Step 3** Click **Save**. Your first simphone and its associated line DN is now configured.

---

**Use Simphone Bulk Administration Tool**

To use the Bulk Administration Tool, you must first import the comma-separated-values template (from either the RSM installation CD or installed instance of RSM), and then edit it, as applicable, in a spreadsheet application such as Microsoft Excel.
Procedure

Step 1 Import the rsmsimphones.csv spreadsheet template file from the installed instance of RSM (located in the C:\CiscoRSM\Extras directory).

Step 2 Open the file in a spreadsheet application, then add or remove rows in the file to match the number of simphone devices you need to create (default rows = 75).

Step 3 If adding new rows, be sure to modify the data in the Device Name and Directory Number 1 columns to increment sequentially from the previous row in the list for the columns (for example, 00005E000001, 00005E000002, 00005E000003, and so on, for the simphone MAC addresses, and 5040, 5041, 5042, and soon, for the line DNs).

Step 4 Verify that the Device Pool, Partition 1, Line CSS 1 and Monitoring Calling Search Space 1 settings are correct for your environment (refer to Tables 3-1 and 3-2, above).

Note No changes are required if you entered RSMSimPhone for the Simphone Device Pool, Partition, and CSS settings during your simphone configuration.

Step 5 Navigate to Bulk Administration > Upload/Download Files.

Step 6 Click Add New.

Step 7 Click Browse and navigate to the rsmsimphones.csv file that you previously downloaded and modified.

Step 8 Choose Phones from the Select the Target drop-down list.

Step 9 Select Insert Phones - All Details from the Select Transaction Type drop-down list.

Step 10 Click Save. The file is uploaded to the system.

Step 11 Navigate to Bulk Administration > Phones > Insert Phones.

Step 12 Select Insert Phones - All Details, and then select rsmsimphones.csv from the File Name drop-down list.

Step 13 Enter Insert RSMSimPhones for the Job Description, and then select Run Immediately.

Step 14 Click Submit. The file is imported into the system.

Step 15 Navigate to Bulk Administration > Job Scheduler to verify that the job status is either Processing or Completed.

Step 16 When the job status is Completed, navigate to Device > Phones and review the phones that you have created.

Step 17 Enter SEP00005E in the Find Phone text box, then click Find. The simphone devices that you have created will appear in the returned results.

Set Up Login Pool Simphone

The first five simphone devices that are created for each cluster are automatically assigned to the VLEngine login pool. The login pool performs a test login to CTI OS when a caller is authenticated by RSM, to support the VLEngine authentication mechanism.

Because CTI OS logins are performed on these simphone devices, they must be associated with the pguser account on each Unified Communications Manager cluster. They must also have Cisco Unified Intelligent Contact Management Enterprise device targets created for them, as described below.
Note

Device target creation is required only for Unified CCE. You do not need to create device targets if you use Cisco Unified System Contact Center Enterprise (Unified SCCE) or if the Cisco Unified CCE PG type is IPCC.

Follow this procedure to associate a pguser.

**Procedure**

**Step 1** Navigate to User Management > Application User.

**Step 2** Click Find to display all application users. Locate then click the pguser account for your cluster.

**Step 3** Select the first five simphone devices in the Device Information > Available Devices list box.

**Step 4** Click the down arrow above the box to move the devices to the Controlled Devices list box. Click Save.

Create RSM User Group

A RSM user group must be created for each cluster used by RSM. This provides the user with the necessary system permissions that would otherwise be available only to the Unified Communications Manager Super Administrator.

Follow this procedure to add an RSM user group to a cluster.

**Procedure**

**Step 1** Navigate to User Management > User Settings > Access Control Group.

**Step 2** Click Add New.

**Step 3** Enter Remote Silent Monitoring in the Name field, then click Save.

**Step 4** Navigate to User Management > User Group.

**Step 5** Click Find to display all user groups.

**Step 6** Click the icon in the Roles column for the Remote Silent Monitoring group.

**Step 7** Click Assign Role to Group. A new window appears.

**Step 8** Click Find to display all group roles.

**Step 9** Select the following roles:

- Standard CTI Allow Call Monitoring
- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

**Step 10** Click Add Selected. The User Group Configuration page appears.

**Step 11** Click Save.
Create RSM Application User

You must create an application user named rsmuser on each Unified Communications Manager cluster for RSM. This user derives its permissions from the user group that was previously created. The rsmuser must be associated with all simphones in the cluster (with the exception of simphones in the login pool). It must also be associated with all agent phones that RSM can monitor.

Simphones in the login pool (that is the first five simphone devices) must be associated with the cluster’s pguser, while all other simphones not in the login pool are associated with the RSM application user.

Note

- For 4000 agent deployment with two PGs, create two Application Users, one for each of the agent PGs.
- Whenever a new non-login-pool simphone or agent device is created, it must be associated with the RSM user.

Follow this procedure to add an RSM application user to a cluster.

Procedure

Step 1 Navigate to User Management > Application User.
Step 2 Click Add New to create a new application user.
Step 3 Enter rsmuser for the user ID.
Step 4 Enter a password. Ensure that the password is alphanumeric and does not contain any special characters.
Step 5 Associate the user with all simphone devices in the cluster (except for the login pool devices) by selecting those devices in the Available Devices section and moving them to the Controlled Devices section.
Step 6 Associate all agent phone devices to be monitored through RSM.
Step 7 From the Permissions Information window, click Add to User Group, and then add the user to the Remote Silent Monitoring group, as previously created.
Step 8 Click Save.

Set Up Agent Phone Device

To configure an agent phone device to be monitored by RSM, ensure the following:

- Edit the device using the Cisco Unified Communications Manager Administration interface and enable the Built-In Bridge setting
- Associate the device with the rsmuser, similar to the way it is associated with the pguser.
Configure Caller-Specific Music on Hold

Upload audio file

Follow this procedure to upload an audio file in an existing node or new node in a Cisco Unified Communications Manager cluster.

If you are uploading to a new node, you must first configure a new and dedicated Music on Hold node that can have only two Cisco Unified Communications Manager services running: Cisco Call Manager, and Cisco IP Voice Media Streaming Application. Additionally, the Cisco IP Voice Media Streaming Application service must be deactivated in all of the other nodes in the Cisco Unified Communications Manager cluster that contains the dedicated Music on Hold node. For more information, see Installing Cisco Unified Communications Manager.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Cisco Unified Communications Manager Administration page.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the Media resources tab, and then click MOH Audio File Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the MOH Audio File Management page, click Upload File.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Upload File window, click Browse, select the audio file that you want to set for Music on Hold, and then click Open.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Upload File.</td>
</tr>
</tbody>
</table>

The audio file is now available for use as a Music on Hold audio source.

What to Do Next

Configure the uploaded audio file so that it can be used as an audio source for Music on Hold.

Configure audio source

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Cisco Unified Communications Manager Administration page, click Media resources tab, and then click Music On Hold Audio Source.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add new.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the MOH Audio Stream Number field, enter a number that you want to assign to the audio file. You cannot choose a number that has already been assigned to another audio file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the MOH Audio Source file drop-down menu, choose the audio file that you want to configure as the MoH audio source.</td>
</tr>
<tr>
<td>Step 5</td>
<td>(Optional) The MOH Audio Source Name field automatically populates the name of the audio file that you chose in the previous step. You can edit the name of the audio file that you selected.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>
What to Do Next
Configure the audio source in the Unified CCE routing script.

Configure Unified CCE routing script

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to the Unified CCE Administrator workstation.</td>
</tr>
<tr>
<td>2</td>
<td>Open the Script Editor.</td>
</tr>
<tr>
<td>3</td>
<td>Open the script in which you want to set the caller specific Music on Hold.</td>
</tr>
</tbody>
</table>
| 4    | Set the call variable `SIPHeader` with the value `X-cisco-moh-source=mod-<User Hold MoH Audio File number>,<Network Hold MoH Audio File number>`.

**Example:**
For example, `X-cisco-moh-source=mod-6,7`; where 6 and 7 are the numbers that you assigned to the audio file. In this example, the audio file assigned for number 6 is played when the call is placed on user hold, and the audio file assigned for number 7 is played when the call is placed on network hold.

**Note**
- List the new call variable after a Dialed Number (DN) or CallingLineID node. This ensures that the call is for a particular DN, or from a particular Calling Line ID.
- If only one audio file is specified, the same file is used for both user hold and network hold.
- If the audio stream that you specified is not present in the Cisco Unified Communications Manager cluster, then the default Music on Hold of the device plays.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

The audio file is now configured as the source audio file that will play for caller specific Music on Hold.

Configure Cisco Finesse

Configure Contact Center Enterprise CTI Server Settings

Access the administration console on the primary Finesse server to configure the A Side and B Side CTI servers.

**Note**
After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to access the Finesse administration console.
If you are using HTTPS, the first time you access the administration console, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

**Procedure**

**Step 1** Sign in to the administration console on the primary Finesseserver:
http://FQDN of Finesse server/cfadmin

**Step 2** Sign in with the Application User credentials defined during installation.

**Step 3** In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Side Host/IP Address</td>
<td>Enter the hostname or IP address of the A Side CTI server. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.</td>
</tr>
<tr>
<td>A Side Port</td>
<td>Enter the port number of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server.</td>
</tr>
<tr>
<td>Peripheral ID</td>
<td>Enter the ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI servers.</td>
</tr>
<tr>
<td>B Side Host/IP Address</td>
<td>Enter the hostname or IP address of the B Side CTI server.</td>
</tr>
<tr>
<td>B Side Port</td>
<td>Enter the port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server.</td>
</tr>
</tbody>
</table>

**Step 4** Click **Save**.

**Configure Contact Center Enterprise Administration & Data Server Settings**

Configure the Contact Center Enterprise Administration & Data Server settings to enable authentication for Finesse agents and supervisors.
Procedure

Step 1  If you are not already signed in, sign in to the administration console.

Step 2  In the Contact Center Enterprise Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the following table. Refer to your configuration worksheet if necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Host/IP Address</td>
<td>Enter the hostname or IP address of the Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Backup Host/IP Address</td>
<td>Enter the hostname or IP address of the backup Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Database Port</td>
<td>Enter the port of the Unified CCE Administration &amp; Data Server.</td>
</tr>
<tr>
<td>AW Database Name</td>
<td>Enter the name of the AW Database (AWDB) (for example, ucceinstance_awdb).</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain of the AWDB.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username required to sign into the AWDB.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password required to sign in to the AWDB.</td>
</tr>
</tbody>
</table>

Step 3  Click Save.

Configure Cluster Settings

Configure the cluster settings for the secondary Finesse node. The secondary Finesse node handles agent requests if the primary server goes down.

Procedure

Step 1  If you are not already signed in, sign in to the administration console with the Application User credentials.

Step 2  In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.

Step 3  Click Save.
Restart Cisco Finesse Tomcat

After you make changes to the Contact Center Enterprise CTI Server, Contact Center Enterprise Administration & Data Server, or cluster settings, restart Cisco Finesse Tomcat for the changes to take effect.

Procedure

Step 1  Access the CLI and run the following command:
        `utilsservicelist`  
Step 2  You can enter the command `utilsservice list` to monitor the Cisco Finesse Tomcat Service. After Cisco Finesse Tomcat changes to STARTED, agents who have passwords can sign in to the desktop.

Check Replication Status

Procedure

Step 1  Access the CLI on the primary Finesse server.
Step 2  Sign in with the Administrator User credentials defined during installation.
Step 3  Run the following command:
        `utilsservice list` 
        This command returns the replication status on both the primary and secondary Finesse servers.

Ensure Agents Have Passwords

Agents who do not have a password defined in Unified CCE Configuration Manager cannot sign in to Finesse. Agent password is an optional field in Unified CCE, but it is mandatory for Cisco Finesse.

For agents who do not have passwords, you must perform the following steps:

Procedure

Step 1  Launch Unified CCE Configuration Manager.
Step 2  Locate the record for the agent (Agent Explorer > Agent tab).
Step 3  Enter a password, and save the record.
Ensure Logout Non-Activity Time for Agents is Configured

The Logout non-activity time specifies how long an agent can remain inactive in the Not Ready state before that agent is signed out of Finesse. Perform the following steps to configure Logout non-activity time for an agent.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the Unified CCE Configuration Manager.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Launch Agent Desk Settings List (Tools &gt; List Tools).</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Agent Desktop Settings from the list.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Logout non-activity time field, enter the number of seconds of agent inactivity while in the Not Ready state before the system software signs the agent out. You can enter a value between 10 seconds and 7200 seconds.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save. The modified settings are applied to all of the agents who use these agent desktop settings.</td>
</tr>
</tbody>
</table>

Ensure Agents Can Sign in to Desktop

After the system administrator defines configuration settings and restarts services, agents who have passwords and operational handsets can sign in to the Finesse Agent Desktop.

**Note**

Finesse agents can use either their loginID or loginName to sign in. Ensure that each agent's loginID and loginName are unique across both sets of data. If one agent's loginID matches another agent's loginName, neither agent can sign in.

**Note**

After you restart Finesse, it takes approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to sign in to the desktop.

**Note**

If you are using HTTPS, the first time you access the agent desktop, you see a browser security warning. To eliminate browser security warnings each time you sign in, you can trust the self-signed certificate provided with Finesse or obtain and upload a CA certificate.

**Procedure**

| Step 1 | Enter the following URL in the address bar of your browser:  
|        | http://FQDN of Finesse server/desktop |
Step 2  If you installed the language pack COP file, you can select the language you want to appear on the desktop from the language selector drop-down list. If you did not install the language pack COP file, the language selector drop-down list does not appear in the user interface.

Note If you installed the language pack COP file, you can also select a language by passing the locale as part of the URL (for example, http://FQDN of Finesse server/desktop?locale=fr_FR) or by changing your browser preferred language. The default language is English (en_US).

Step 3  Enter your agent ID or username, password, and extension, and the click Sign In.

Figure 3: Desktop Sign-In

Trust Self-Signed Certificate

Trust the self-signed certificate provided by Finesse to eliminate browser warnings each time you sign in to the administration console or agent desktop.

If you are not using HTTPS or if you uploaded a CA certificate, you can skip this procedure.

Procedure

Step 1  In your browser, enter the URL for the administration console (https://FQDN of the primary Finesse server/cfadmin) or the agent desktop (https://FQDN of the primary Finesse server/desktop).

Step 2  Perform the steps in the following table for the browser you are using.
1 A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)**. This action opens the sign in page for the administration console (or agent desktop). A certificate error appears in the address bar of your browser.

2 Click **Certificate Error**, and then click **View Certificates** to open the Certificate dialog box.

3 On the Certificate dialog box, click **Install Certificate**. This action opens the Certificate Import Wizard.

   **Note** If you use Internet Explorer 11 with Windows 8.1, you must add Finesse to your trusted sites before the Install Certificate option appears (**Internet Options > Security > Trusted Sites > Sites**).

   After you click **Install Certificate**, under **Store Location**, select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users who use this computer.

4 Click **Next**.

5 Select **Place all certificates in the following store**, and then click **Browse**.

6 Select **Trusted Root Certification Authorities**, and then click **OK**.

7 Click **Next**.

8 Click **Finish**.

9 If a Security Warning dialog box appears that asks if you want to install the certificate, click **Yes**.

   A Certificate Import dialog box that states the import was successful appears.

10 Click **OK**.

11 Enter your credentials, and then click **Sign In**.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| If you use Firefox: | 1. A page appears that states this connection is untrusted.  
2. Click **I Understand the Risks**, and then click **Add Exception**.  
3. On the Add Security Exception dialog box, ensure the **Permanently store this exception** check box is checked.  
4. Click **Confirm Security Exception**.  
   The page that states this connection is untrusted automatically closes and the administration console (or agent desktop) loads.  
5. Enter your credentials, and then click **Sign In**.  
6. For the agent desktop only, an error appears that states Finesse cannot connect to the Cisco Finesse Notification Service and prompts you to add a security exception for the certificates issued by the Finesse server. Click **OK**. |

---

**Obtain and Upload CA Certificate**

**Note**

This procedure only applies if you are using HTTPS.

This procedure is optional. If you are using HTTPS, you can choose to obtain and upload a CA certificate or you can choose to use the self-signed certificate provided with Finesse.

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a Certificate Authority (CA). Use the Certificate Management utility from Cisco Unified Communications Operating System Administration.

To open Cisco Unified Communications Operating System Administration, enter the following URL in your browser:

https://FQDN of primary Finesse server:8443/cmplatform

Sign in using the username and password for the Application User account created during the installation of Finesse.

**Note**

You can find detailed explanations in the Security topics of the *Cisco Unified Communications Operating System Administration Online Help*.

**Procedure**

**Step 1** Generate a CSR.
a) Select **Security > Certificate Management > Generate CSR.**
b) From the Certificate Name drop-down list, select **tomcat.**
c) Click **Generate CSR.**

**Step 2**
Download the CSR.
a) Select **Security > Certificate Management > Download CSR.**
b) From the Certificate Name drop-down list, select **tomcat.**
c) Click **Download CSR.**

**Step 3**
Generate and download a CSR for the secondary Finesses server.
To open Cisco Unified Operating System Administration for the secondary server, enter the following URL in the address bar of your browser:
https://FQDN of secondary Finesses server:8443/cmplatform

**Step 4**
Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.
**Note** To set up the certificate chain correctly, you must upload the certificates in the order described in the following steps.

**Step 5**
When you receive the certificates, select **Security > Certificate Management > Upload Certificate.**

**Step 6**
Upload the root certificate.
a) From the Certificate Name drop-down list, select **tomcat-trust.**
b) In the Upload File field, click **Browse** and browse to the root certificate file.
c) Click **Upload File.**

**Step 7**
Upload the intermediate certificate.
a) From the Certificate Name drop-down list, select **tomcat-trust.**
b) In the Root Certificate field, enter the name of the root certificate that you uploaded in the previous step.
Do not include the extension (for example, TEST Root CA 2048).
c) In the Upload File field, click **Browse** and browse to the intermediate certificate file.
d) Click **Upload File.**

**Step 8**
Upload the application certificate.
a) From the Certificate Name drop-down list, select **tomcat.**
b) In the Root Certificate field, enter the name of the intermediate certificate that you uploaded in the previous step. Include the .pem extension (for example, TEST-SSL-CA.pem).
c) In the Upload File field, click **Browse** and browse to the application certificate file.
d) Click **Upload File.**

**Step 9**
After the upload is complete, sign out of Finesses.

**Step 10**
Access the CLI on the primary Finesses server.

**Step 11**
Enter the command **utilsservicerestartCiscoFinessesNotificationService** to restart the Cisco Finesses Notification service.

**Step 12**
Enter the command **utilsservicerestartCiscoFinessesTomcat** to restart the Cisco Finesses Tomcat service.

**Step 13**
Upload the application certificate to the secondary Finesses server.
You do not need to upload the root and intermediate certificates to the secondary Finesses server. After you upload these certificates to the primary server, they are replicated to the secondary server.

**Step 14**
Access the CLI on the secondary Finesses server and restart the Cisco Finesses Notification Service and the Cisco Finesses Tomcat Service.
Configure DNS on Clients

**Note**

This procedure is required for uncommon environments where non-hierarchical DNS configuration exists. If your environment has hierarchical DNS configuration, you do not need to perform this procedure. This procedure applies to clients that use a Windows operating system. For information about configuring DNS on Mac clients, see your Apple documentation (www.apple.com/mac).

Configuring DNS on client computers allows the clients to resolve the fully-qualified domain name (FQDN) of the active Finesse server during a failover.

**Procedure**

**Step 1** Go to Control Panel > Network and Internet > Network and Sharing Center. (Open the Control Panel, enter Network Connections in the search bar, and then click View network connections.)

**Step 2** Click the appropriate network connection. A dialog box showing the status of the connection appears.

**Step 3** Click Properties.

**Step 4** On the Networking tab, select Internet protocol version 4 (TCP/IPv4) or Internet protocol version 6 (TCP/IPv6) if the client is IPV6, and then click Properties.

**Step 5** Click Advanced.

**Step 6** On the DNS tab, under DNS server addresses, in order of use, click Add.

**Step 7** Enter the IP address of the DNS server that was entered during installation and click Add.

**Step 8** If a secondary DNS was entered during installation, repeat Step 5 and Step 6 to add its IP address.

Live Data Reports

Cisco Unified Intelligence Center provides Live Data real-time reports that you can add to the Finesse desktop.

**Prerequisites for Live Data**

Before you add Live Data reports to the desktop, you must meet the following prerequisites:

- You must have the Live Data reports configured and working in Cisco Unified Intelligence Center.

- You must use either HTTP or HTTPS for both Cisco Unified Intelligence Center and Finesse. You cannot use HTTP for one and HTTPS for the other. The default setting for both after a fresh installation is HTTPS. If you want to use HTTP, you must enable it on both Cisco Unified Intelligence Center and Finesse. For information about enabling HTTP for Cisco Unified Intelligence Center, see the Administration Console User Guide for Cisco Unified Intelligence Center at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
• Ensure that user integration synchronization is enabled for Cisco Unified Intelligence Center. For more information, see the Administration Console User Guide for Cisco Unified Intelligence Center.

• If your deployment uses HTTPS, you must upload security certificates to the Finesse, Cisco Unified Intelligence Center, and Live Data servers depending your deployment:

<table>
<thead>
<tr>
<th>On Server</th>
<th>Import Certificates From</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finesse</td>
<td>Live Data and Cisco Unified Intelligence Center</td>
</tr>
<tr>
<td>Live Data</td>
<td>None required</td>
</tr>
<tr>
<td>Cisco Unified Intelligence Center</td>
<td>Live Data</td>
</tr>
</tbody>
</table>

Finesse, Cisco Unified Intelligence Center, and Live Data are installed with self-signed certificates. However, if you use the self-signed certificates, agents and supervisors must accept certificates in the Finesse desktop when they sign in before they can use the Live Data gadget. To avoid this requirement, you can provide a CA certificate instead. You can obtain a CA certificate from a third-party certificate vendor or produce one internal to your organization.

**Add Live Data Reports to Finesse**

The following sections describe how to add the Live Data reports to the Finesse desktop. The procedure that you follow depends on several factors, described in the following table.

<table>
<thead>
<tr>
<th>Procedure</th>
<th>When to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Live Data reports to default desktop layout</td>
<td>Use this procedure if you want to add Live Data reports to the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.</td>
</tr>
<tr>
<td>Add Live Data reports to custom desktop layout</td>
<td>Use this procedure if you have customized the Finesse desktop layout.</td>
</tr>
<tr>
<td>Add Live Data reports to team layout</td>
<td>Use this procedure if you want to add Live Data reports to the desktop layout for specific teams only.</td>
</tr>
</tbody>
</table>

**Add Live Data Reports to Default Desktop Layout**

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the default desktop layout. Use this procedure after a fresh installation of Finesse. If you upgraded Finesse but do not have a custom desktop layout, click **Restore Default Layout** on the Manage Desktop Layout gadget and then follow the steps in this procedure. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.
Procedure

Step 1  Sign into the Finesse administration console (https://FQDN of Finesse server/cfadmin), in which FQDN refers to the fully qualified domain name.

Step 2  Click the Desktop Layout tab.

Step 3  Remove the comment characters (<!-- and -->) from each report that you want to add to the desktop layout. Make sure you choose the reports that match the method your agents use to access the Finesse desktop (HTTP or HTTPS).

Step 4  Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 5  Optionally, change the gadget height.

Example:
The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows, replacing 310 with 400:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=400&viewId_1=99E6C8E210000141000000D8A0006C4&
filterId_1-agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
filterId_2-agent.id=CL%20teamName
</gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 6  Click Save.

Note  After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Add Live Data Reports to Custom Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to a custom desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.
## Procedure

**Step 1** Sign into the Finesse administration console.

**Step 2** Click the **Desktop Layout** tab.

**Step 3** Click **Finesse Default Layout XML** to show the default layout XML.

**Step 4** Copy the XML code for the report you want to add from the Finesse default layout XML. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

### Example:

To add the Agent Report for HTTPS, copy the following:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E21000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName
viewId_2=9AB7848B1000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
```

**Step 5** Paste the XML within the tab tags where you want it to appear.

### Example:

To add the report to the home tab of the agent desktop:

```xml
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E21000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName
viewId_2=9AB7848B1000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

**Step 6** Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

**Step 7** Optionally, change the gadget height.

### Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the `gadgetHeight` parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=400&viewId_1=99E6C8E21000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B1000141000001C50A0006C4&
filterId_2=agent.id=CL%20teamName
</gadget>
```
To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

**Step 8** Click **Save**.

**Note** After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

---

**Add Live Data Reports to Team Layout**

The Finessedefault layout XML contains commented XML code for the Live Data report gadgets available for the Finessedeskopt. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the desktop layout of a specific team. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

**Procedure**

**Step 1** Sign in to the Finessedadministration console.

**Step 2** Click the **Desktop Layout** tab.

**Step 3** Click **Finessedefault Layout XML** to show the default layout XML.

**Step 4** Copy the XML code for the report you want to add from the Finessedefault layout XML. If your agents use HTTP to access Finessesi, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

**Example:**

To add the Agent Report for HTTPS, copy the following:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB784B10000141000001C50A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

**Step 5** Click the **Team Resources** tab.

**Step 6** Select the team from the list of teams for which you want to add the report.

**Step 7** In the Resources for `<team name>` area, click the **Desktop Layout** tab.

**Step 8** Check the **Override System Default** check box.

**Step 9** Paste the XML within the tab tags where you want it to appear.

**Example:**
To add the report to the home tab of the agent desktop:

```xml
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6CB210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&
        viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
      <label>finesse.container.tabs.agent.manageCallLabel</label>
    </tab>
  </tabs>
</layout>
```

**Step 10** Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

**Step 11** Optionally, change the gadget height.

**Example:**
The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
  gadgetHeight=400&viewId_1=99E6CB210000141000000D80A0006C4&
  filterId_1=agent.id=CL%20teamName&
  viewId_2=9AB7848B10000141000001C50A0006C4&
  filterId_2=agent.id=CL%20teamName
</gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

**Step 12** Click Save.

**Note** After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

---

**Modify Live Data Stock Reports for Finesse**

This procedure describes how to modify the Live Data stock reports in Cisco Unified Intelligence Center and add the modified report to the Finesse desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.
To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Cisco Unified Intelligence Center.

**Procedure**

**Step 1** Sign in to the Finesse administration console.
**Step 2** Click the Desktop Layout tab.
**Step 3** Click Finesse Default Layout XML to show the default layout XML.
**Step 4** Copy the gadget URL for the report you want to modify from the Finesse default layout XML and paste it into a text editor.

**Example:**
If you want to modify the Agent Report for HTTPS, copy the following URL and paste it into a text editor:

```xml
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B1000014100000001C50A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

**Step 5** In Cisco Unified Intelligence Center, in Edit view of the report, select the view for which you want to create a gadget URL and then click Links.
The HTML Link field displays the permalink of the customized report.

**Step 6** Copy the permalink of the customized report from the HTML Link field, and paste it in a text editor. Then copy the viewId value from this link into the desired view.

**Example:**
Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htm?viewId=5C90012F1000014000000830A4E5B33&linkType=htmlType&viewType=Grid
```

**Step 7** Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.
**Step 8** Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.
**Step 9** Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click Save.

**Note**
After you add the gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without the need to scroll.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.
### Initial Configuration Troubleshooting

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>The administration console does not load after a fresh installation.</td>
<td>1 Clear your browser cache (delete browsing history and cookies).</td>
</tr>
<tr>
<td></td>
<td>2 If the problem persists, restart the Cisco Finesse Tomcat service or restart the Finesse server.</td>
</tr>
<tr>
<td>If</td>
<td>Then</td>
</tr>
<tr>
<td>----</td>
<td>------</td>
</tr>
</tbody>
</table>
| Agents cannot sign in to the desktop after a fresh installation. | 1 Verify that the agent ID and password are correct.  
  **Note** Finesse agents can use either their `loginID` or `loginName` to sign in. Ensure that each agent's `loginID` and `loginName` are unique across both sets of data. If one agent's `loginID` matches another agent's `loginName`, neither agent can sign in.  
  2 Verify that a valid domain was configured during installation and that forward and reverse DNS are set up correctly. To check whether DNS was configured during installation, check the `install.log` for the following:  
  `InstallWizard|USER_ACTION_BTN_PUSH: Screen=DNS Client Configuration, button pushed = No|<LVL::Info`  
  The preceding message indicates that DNS was not configured during the installation. Reinstall Finesse and configure the DNS with a valid domain.  
  3 Verify that the agent is configured in Unified CCE.  
  4 Verify that the AWDB is configured correctly.  
  a Check the `realm.log` for the following line:  
  "ERROR  
  com.cisco.ccbu.finesse.realms.ccerealm.CCERealmConfig - Cannot connect to any AWDB! Ensure that at least one AWDB is configured properly and running!"  
  This line indicates that Finesse cannot connect to the AWDB.  
  b Check that the values entered in the Contact Center Enterprise Administration & Data Server Settings gadget are correct.  
  • Verify that the username entered is a Windows domain user.  
  • Verify that the username is not prepended with the domain (for example, `domain\username`).  
  • Verify that the port configured is open to the Finesse server.  
  c Check that the AWDB is set up correctly and running.  
  • The AWDB SQL server must use Windows authentication.  
  • Verify that the AWDB server is up and that the Distributor service is running.  
  5 Restart Cisco Finesse Tomcat on the primary and secondary Finesse servers.  
  6 Verify that the agent's device is properly configured in Unified Communications Manager and is active. |
Upgrade Overview

- Multistage Upgrades and Maintenance Windows, page 167
- Unified CCE Contact Center Upgrade Flowcharts, page 170
- Data Migration Considerations, page 177
- Silent Upgrade, page 178
- Uninstallation, page 178

Multistage Upgrades and Maintenance Windows

A Unified CCE solution upgrade likely involves a multistage process; components are grouped in several stages for upgrading. At each stage in the upgrade, the upgraded components must interoperate with components that have not yet been upgraded to ensure the overall operation of the contact center. Therefore, it is important to verify this interoperability during the planning stages of the upgrade.

Before upgrading a production system, perform the upgrade on a lab system that mirrors your production system to identify potential problems safely.

The following table details the required sequence for upgrading Unified CCE solution components, and the minimum component groupings that must occur together within one stage. Follow each stage to completion within one maintenance window. Each maintenance window must accommodate any testing required to ensure system integrity and contact center operation.

You can combine more than one complete stage into a single maintenance window, but you cannot break any one stage into multiple maintenance windows.

Note

- If you have installed Cisco Agent Desktop (CAD) on a PG machine, you must upgrade the CAD to the latest supported version before you upgrade the PG machine to Unified CCE 11.0(x).
- Unified CCE 11.0(x) does not support SQL Server 2008. If CAD is currently running on SQL Server 2008, upgrade to SQL 2014 before attempting to upgrade the PG to CCE 11.0(x).

Upgrade the components that apply to your Unified CCE contact center as follows:
### Multistage Upgrades and Maintenance Windows

#### Upgrade Overview

<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Agent and supervisor desktops</td>
<td>• Cisco Finesse</td>
<td>If you use the CTI OS or the Cisco Agent Desktops, you must upgrade them in a later window.</td>
</tr>
<tr>
<td>2</td>
<td>Queuing and self-service</td>
<td>• Cisco Unified Customer Voice Portal (CVP) (Operations Console, Reporting Server, Call Server/VXMLServer, Unified Call Studio)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Gateways</td>
<td>• IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 6.) • CVP VXML Gateways</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Reporting server</td>
<td>• CUIC server</td>
<td>If upgraded without upgrading reporting templates at the same time, is backwards compatible with previous Central Controller version.</td>
</tr>
<tr>
<td>5</td>
<td>Central Controller</td>
<td>• Unified CCE Router • Unified CCE Logger • Admin &amp; Data server (AW/HDS/DDS) • CUIC Reporting Templates • CCMP • Administration Client</td>
<td>You can upgrade Side A and Side B in different maintenance windows, but you must upgrade all central controller components on one side together.</td>
</tr>
<tr>
<td>Stage</td>
<td>Component Group</td>
<td>Components</td>
<td>Notes</td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| 6     | Peripherals    | • Agent (Unified Communications Manager) PG or System PG, plus  
* CTI Server  
* CTI OS Server  
* Outbound Option Dialer and SIP IOS Gateway  
* Remote Silent Monitor  
* VRU PG (if collocated with Agent PG on VM)  
* MR PG (if collocated with Agent PG on VM), plus  
  * EIM/WIM  
* Unified CCE Gateway PG (if collocated with Agent PG on VM) | Everything that resides on one virtual machine must be upgraded together.  
You can have many PGs located on different virtual machines.  
You can upgrade each PG virtual machine in its own maintenance window. |
| 7     | Peripherals    | • MR PG (if not collocated with Agent PG on VM), plus  
  * EIM/WIM  
* VRU PG (if not collocated with Agent PG on VM)  
* Unified CCE Gateway PG (if not collocated with Agent PG on VM)  
* CRM connector | You can have many PGs located on different virtual machines.  
You can upgrade each PG virtual machine in its own maintenance window. |
| 8     | Agent desktop client software | • CTI OS (Agent/Supervisor Desktops)  
or  
• CAD (Agent/Supervisor Desktops) | You can have many desktops located in many different sites.  
You can upgrade CTI OS or CAD desktops in multiple maintenance windows; the later upgrade stages are not dependent on the completion of this stage. |

Note: The CTI Toolkit Desktop and Cisco Agent Desktop are deprecated in Unified CCE Release 11.0(1). Do not include these desktops in new deployments. Support for these desktops will be removed in a future release.
### Unified CCE Contact Center Upgrade Flowcharts

The following diagram illustrates the solution-level upgrade flow for a Cisco Unified Contact Center Enterprise solution upgrade.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Call Processing</td>
<td>• Cisco Unified Communications Manager (Unified Communications Manager)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• JTAPI on Agent (Unified Communications Manager) PG</td>
<td></td>
</tr>
<tr>
<td>Any (See Notes)</td>
<td>Media Recording</td>
<td>• MediaSense</td>
<td>MediaSense is a standalone application that you can upgrade at any time after IOS Gateway upgrades.</td>
</tr>
</tbody>
</table>

*If you are using Unified IP IVR for self-service and queueing, see Getting Started with Cisco Unified IP IVR.*
The following diagrams illustrate the stages of the component-level upgrade flows for a Cisco Unified Contact Center Enterprise solution upgrade. Each diagram covers one of the stages. The letter at the end of each flow indicates the start of the next flow that you should perform.
Upgrade Overview

Unified CCE Contact Center Upgrade Flowcharts

1. Obtain licenses for this release
   - Back up server registry, databases
     - New domain?
       - yes
         - Migrate Active Directory and DNS to non-UnifiedCCE servers
       - no
         - Temp A&D servers required for continuity of configuration and reporting?
           - yes
             - Export Active Directory users
           - no
             - Set up temp A&D servers
     - Disable configuration changes

The diagram illustrates the steps involved in upgrading the Cisco Unified Contact Center Enterprise, starting with obtaining licenses and progressing through the necessary preparations and changes to ensure a smooth transition to the new release.
Data Migration Considerations

The data migration set is identical irrespective of the migration path you choose to follow.

The Technology Refresh task involves:

- Backup/Restore the data
- Data migration

The Common Ground upgrade task involves only data migration.

For Technology Refresh upgrades, have the fastest possible network (gigabit through one network switch) between the source and the destination machines. Use of a crossover cable is not supported because it lacks buffer memory and can cause data loss.

To reduce data migration time, consider reducing the database size by taking the following steps:

- Remove redundant records, especially call detail records (RCD, RCV, TCD, and TCV tables). However, be aware that removing records affects the availability of historical reports; knowledge of the HDS schema is required.
- Purge the Logger database of all data that is already replicated to the HDS (25 GB or less).
- Use more efficient hardware, especially on I/O subsystems:
  - RAID 1 + 0
  - I/O Cache – more is better

Enable the Tempdb log to expand up to 3 GB.

Time Guidelines and Migration Performance Values

The closest estimate of time and space requirement is generated by running EDMT against a copy of your production database, on hardware that is similar to your production environment, in a lab environment. For customers who do not have the facility, the following sections provide information gathered while performance testing in the labs at Cisco Systems, Inc.

- **Typical database migration performance values:** The following table provides high level guidelines for the time taken to upgrade the Loggers and HDSs based on the hardware (as defined in the Virtualization for Unified CCE at [http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE](http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE)), and the results observed during internal upgrade testing with hardware C210 M2. Actual times may vary based on the parameters previously mentioned.
• **Backup and Restore - Technology Refresh only**: The backup speed depends on the speed of the network, and the speed of the disk sub-system. The faster the network, the sooner the network copy.

<table>
<thead>
<tr>
<th>Database Used Size (GB)</th>
<th>Backup Time (hours)</th>
<th>Restore Time (minutes)</th>
<th>Data Migration Time (minutes)</th>
<th>Total Time (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.5 - 1.5</td>
<td>5 - 15</td>
<td>&lt;1</td>
<td>0.5 - 1.5</td>
</tr>
<tr>
<td>30</td>
<td>2.5 - 3.5</td>
<td>10 - 20</td>
<td>&lt;2</td>
<td>3 - 4</td>
</tr>
<tr>
<td>70</td>
<td>7 - 8</td>
<td>20 - 45</td>
<td>&lt;5</td>
<td>8 - 9</td>
</tr>
</tbody>
</table>

**Note**

- The values in the Database Used Size column are based on the amount of disk space used by the source database, and not the size of the disk it resides on.
- The values in the Backup Time and Restore Time columns assumes that the network meets the minimum requirements. For more information about the minimum requirements, refer to the Virtualization for Unified CCE at [http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE](http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE).
- For Technology Refresh upgrades, have the fastest network possible (gigabit through one network switch) between the source and the destination machines. Use of a crossover cable is not supported because it lacks buffer memory and can cause data loss.

---

### Silent Upgrade

There are situations where a silent upgrade is preferable to running an installation wizard. You can run a silent installation when performing a fresh install or an upgrade.

For information, see the Installation section of this document.

### Uninstallation

Unified CCE supports the uninstall option from the Windows Add/Remove option. This option removes the patches, base version files, and the related registry. The option also removes Unified CCE component software installed by the ICM-CCE-CCHInstaller.

However, it does not remove the following:

- Java Runtime Environment
- Unified CCE databases

Reinstallation is also supported. To reinstall, rerun the ICM-CCE-CCHInstaller.
After you upgrade Unified CCE to a new version, you cannot rollback to a previous version. The option to rollback is only available with maintenance releases.
Common Ground Upgrade

• Preupgrade Overview, page 181
• Common Ground Preupgrade Task Flow, page 182
• Common Ground Preupgrade Tasks, page 183
• Upgrade Overview, page 186
• Common Ground Upgrade Task Flow, page 189
• Common Ground Upgrade Tasks, page 192

Preupgrade Overview

The preupgrade process ensures that your systems have the necessary software to support your contact center. These tasks prepare the way for a successful upgrade of your Cisco contact center components to the new release.

Preupgrade Tools

During the preupgrade process, use the following tools as required:

• User Migration Tool—A standalone Windows command-line application used for all upgrades that involve a change of domain. The tool exports all existing user accounts (config/setup and supervisors) in the source domain into a flat file. The file is used in the target domain during the upgrade.

  You can download the User Migration Tool from Cisco.com by clicking ICM User Migration Tool Software.

• Regutil Tool—Used in Technology Refresh upgrades, exports the Cisco Systems, Inc. registry from the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

  You can download the Regutil Tool from Cisco.com by clicking Contact Center Enterprise Tools.

• Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.

  The ICMDBA Tool is delivered with the main installer.
- Domain Manager—Used to provision Active Directory.
The Domain Manager Tool is delivered with the main installer.

Common Ground Preupgrade Task Flow

Perform the following Common Ground preupgrade tasks in any order.

Note

The Common Ground upgrade assumes the host server runs on Windows Server 2012 R2.

<table>
<thead>
<tr>
<th>Task</th>
<th>Release 10.0 to 11.0</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESX Supportability</td>
<td>yes</td>
<td>ESX Supportability, on page 183</td>
</tr>
<tr>
<td>Disaster Recovery Plan</td>
<td>yes</td>
<td>Disaster Recovery Plan, on page 184</td>
</tr>
<tr>
<td>Change the SCSI Controller Type</td>
<td>yes</td>
<td>Change the SCSI Controller Type, on page 184</td>
</tr>
<tr>
<td>Upgrade VM Network Adapters from E1000 to VMXNet3</td>
<td>yes</td>
<td>Upgrade VM Network Adapters from E1000 to VMXNet3, on page 185</td>
</tr>
<tr>
<td>VM Hardware Version Upgrade</td>
<td>yes</td>
<td>VM Hardware Version Upgrade, on page 186</td>
</tr>
<tr>
<td>Download the Enhanced Database Migration Tool</td>
<td>yes</td>
<td>Upgrade Overview, on page 186</td>
</tr>
<tr>
<td>Back up the server registry</td>
<td>yes</td>
<td>Use your established processes</td>
</tr>
<tr>
<td>Copy ICM directory on all system nodes</td>
<td>yes</td>
<td>Use your established processes</td>
</tr>
<tr>
<td>Task</td>
<td>Release 10.0 to 11.0</td>
<td>See</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Run the following and save the results:</td>
<td>yes</td>
<td>Use your established</td>
</tr>
<tr>
<td>ipconfig -all</td>
<td></td>
<td>processes</td>
</tr>
<tr>
<td>route print -p</td>
<td></td>
<td></td>
</tr>
<tr>
<td>netstat -a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create bootable image of operating system and network configuration</td>
<td>yes</td>
<td>Use your established</td>
</tr>
<tr>
<td>Back up Logger, HDS, BA databases using Microsoft SQL Server Backup</td>
<td>yes</td>
<td>processes</td>
</tr>
<tr>
<td>and Restore utility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If moving to a new domain, migrate Active Directory and DNS to</td>
<td>yes</td>
<td>Migrate Active Directory</td>
</tr>
<tr>
<td>non-Unified CCE servers (Optional)</td>
<td></td>
<td>and DNS, on page 223</td>
</tr>
<tr>
<td>If moving to a new domain, export Active Directory users (Optional)</td>
<td>yes</td>
<td>Migrate Active Directory</td>
</tr>
<tr>
<td>Notify all stakeholders, including:</td>
<td>yes</td>
<td>and DNS, on page 223</td>
</tr>
<tr>
<td>• Cisco Technical Assistance Center (TAC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Local Cisco Representatives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Customer Operations and Emergency Management Center</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Third-party vendors as applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remove DB-lib key from</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>HKEL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSSQLServer\Client\DB-Lib</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Common Ground Preupgrade Tasks**

**ESX Supportability**

Only ESXi version 5.5 is supported for UCCE 11.0(1), However ESXi 5.1 can be used for intermediate upgrade for 10.0(x) Customers.

For example, If a 10.0 customer upgrades an ESXi from 5.0 to 5.5 and gets in to a disaster while doing 11.0(1) common ground upgrade, then when they revert to 10.0 they will end up using 10.0 UCCE with ESX 5.5 which is never supported. To avoid this, we suggest 10.0 customers who ever in ESX 5.0 to upgrade first to 5.1 and post successful 11.0(1) CG migration, they can upgrade the ESXi to 5.5.
Disaster Recovery Plan

Before you start the upgrade process, take a snapshot of the virtual machines on which you are performing an upgrade. Take the snapshot with the VM powered off to reduce the size of the snapshots and post successful migration to UCCE 11.0(1). Snapshots have to be removed to avoid performance impacts.

It's preferred to take a backup of Virtual Machine OVA as well. In case of Snapshot reversal failure, We still have one more backup.

Change the SCSI Controller Type

LSI Logic Parallel is not supported with Windows Server 2012. If the virtual machine has SCSI Controller type as LSI Logic Parallel, you must change it to LSI Logic SAS.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Ensure the virtual machine is powered on.</td>
</tr>
</tbody>
</table>
| Step 2 | Add a new hard disk to the virtual machine.  
When choosing the Virtual Device Node, select SCSI (1:0) and hard disk size as 1MB.  
**Note** When the new virtual disk is created, it creates a second virtual SCSI controller.  
**Caution** Do not click OK at this stage to confirm the changes. |
| Step 3 | Select the second virtual SCSI controller, and then click Change Type. |
| Step 4 | Select the LSI Logic SAS radio button, and then click OK. |
| Step 5 | Click OK to confirm the changes.  
Log in to the virtual machine.  
The operating system automatically detects the new SCSI controller and adds the driver for LSI Logic SAS. |
| Step 6 | In Device Manager, under Storage controllers, ensure that the controller is listed as LSI Adapter SAS 3000 Series.  
Power down the virtual machine.  
Remove the newly added virtual disk. Ensure that you select the Remove from virtual machine and delete files from disk option.  
Selecting this option purges the new disk from the data store.  
The controller is removed automatically. |
| Step 10 | Change the first virtual controller to the LSI Logic SAS setting.  
Power on the virtual machine.  
Usually, Windows displays a message telling you to restart the virtual machine for the changes to take effect.  
If this message is not displayed, restart the virtual machine manually. |
Upgrade VM Network Adapters from E1000 to VMXNet3

Before you upgrade the VM's operating system from Windows Server 2008 R2, upgrade the VM network adapters to VMXNet3. Unified CCE 11.0(1) requires VMXNet3 network adapters. If you upgrade the operating system to Windows Server 2012 R2 without upgrading to VMXNet3, the static IP configuration on the ethernet adapter resets to automatic after the Windows upgrade.

Note
VMware deprecated support for E1000 Ethernet Controllers in ESXi 5.5: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2056935

Procedure

Step 1 Ensure the VMware Tools are Installed.

Step 2 Record the public and private network settings, including the IP addresses, Subnet masks, Default Gateway, DNS, Persistent Static Routes, and so on.

Important You need these values to recreate the configurations on the new virtual machine network adapters.

Step 3 Stop the Unified CCE services. The services cannot be active during reconfiguration of the network adapters.


Step 5 Disable the E1000 public network adapter.

Step 6 Disable the E1000 private network adapter, if the VM has a PG, Router, or Logger.

Step 7 Remove the E1000 public network adapter:
   a) Shut down the operating system of the VM.
   b) Select Edit Settings from the VM context menu.
   c) Select the E1000 public network adapter on the Hardware tab.
   d) Click Remove and then click Finish.
   e) Start the VM.

Step 8 Remove the E1000 private network adapter from VMs for PGs, Routers, and Loggers:
   a) Shut down the operating system of the VM.
   b) Select Edit Settings from the VM context menu.
   c) Select the E1000 public network adapter on the Hardware tab.
   d) Click Remove and then click Finish.
   e) Start the VM.

Step 9 Remove ghosted network adapters
   a) Run this in cmd prompt 'set devmgr_show_nonpresent_devices=1' and press Enter.
   b) Launch Device manager using this cmd'start devmgmt.msc' .
   c) In Device Manager, Click View and select show hidden device.
   d) Expand Network Adapter and uninstall the dimmed E1000 network adapters.

Step 10 Add the VMXNet 3 public network adapter:
   a) Select Edit Settings from the VM context menu.
b) Click **Add** on the Hardware tab.
c) Select **Ethernet Adapter** in the Device Type page and click **Next**.
d) Select **VMXNet 3** from the Adapter Type drop-down list.
e) Select the public network port group from the Network label drop-down list and click **Next**.
f) Click **Finish**.

**Step 11** Add the VMXNet 3 private network adapter to VMs for PGs, Routers, and Loggers:
   a) Select **Edit Settings** from the VM context menu.
   b) Click **Add** on the Hardware tab.
   c) Select **Ethernet Adapter** in the Device Type page and click **Next**.
   d) Select **VMXNet 3** from the Adapter Type drop-down list.
   e) Select the public network port group from the Network label drop-down list and click **Next**.
   f) Click **Finish**.

**Step 12** Apply the network settings that you recorded in Step 1 from the E1000 public and private network adapters to the VMXNet 3 public and private network adapters.

**Step 13** Enable the VMXNet 3 public and private network adapters.

**Step 14** Add the persistent static routes to the Windows Server 2008 R2 on the VM.

**Step 15** Use traceroute to test the connectivity for the public and private networks.

**Step 16** Re-enable the unified CCE services.

---

**VM Hardware Version Upgrade**

In the Vsphere Client, ensure that you have upgraded the VM hardware version to 9. Download VMware Vsphere Powercli tool and use it to complete this procedure. Ensure the VM is powered off during this procedure.

**Procedure**

**Step 1** Connect to the ESX using VMware VSphere PowerCli "Connect-VIServer -Server ESXIP -Protocol https -User username -Password password".

**Step 2** Run command Get-VM "<VM name>" | Set-VM -Version "v9" to change the VM version.

---

**Upgrade Overview**

**Unified CCE Redundant Central Controller Upgrade Flow**

The Unified CCE central controller consists of the Logger, Router, and Administration & Data Server. When upgrading the Unified CCE portion of your contact center, the central controller is upgraded before the other Unified CCE components. While one side (Side A or B) of the redundant system is being upgraded, the other side (Side A or B) operates in stand-alone mode.
For redundant systems, the general flow for upgrading the Unified CCE central controller is as follows:

1. Upgrade the Logger, Router, and Administration & Data Server on Side A.
2. Bring Side A into service and verify the operation. Side B is brought down as Side A is coming into service.
3. Upgrade the Logger, Router, and Administration & Data Server on Side B.
4. Bring Side B into service and verify that duplexed operation begins.

**Update VM Properties**

Rather than recreate the VMs from the new version of the OVA, you can manually update the VM properties to match the new OVA. After you upgrade the vSphere ESXi and before you upgrade the Unified CCE components, update the properties of each VM to match the appropriate OVA, as follows:

1. Determine the version of the OVA from which you created the VM.
2. Update the properties of each VM to match the properties of the appropriate OVA. Check the Virtualization for Unified CCE DocWiki at [http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE](http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE) for descriptions of each OVA.
3. Stop the VM.
4. Edit the properties of the VM to match the properties from the new version of the OVA. Save your changes.
5. Restart the VM.

⚠️ **Caution**

Be careful when you upgrade the virtual machine network adapters. Done incorrectly, this upgrade can compromise the fault tolerance of your contact center.


**SQL Security Hardening**

You can optionally apply SQL security hardening when running the installer. If your company employs custom security policies, bypass this option. Most other deployments benefit from SQL security hardening.

**Upgrade Tools**

During the upgrade process, use the following tools as required:

- **ICM-CCE-CCHInstaller**—The main Unified CCE Installer. It copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.

⚠️ **Note**

Optionally, you can update the JRE installed by the Unified CCE Installer with a later version of the JRE. See [Update the Java Runtime Environment (Optional)](#) on page 57.

You cannot run the installer remotely. Mount the installer ISO file only to a local machine.
Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.

Domain Manager—Used to provision Active Directory.

Web Setup—Used to set up the Call Routers, Loggers, and Administration & Data Servers.

Peripheral Gateway Setup—Used to set up PGs, the CTI server, and the Outbound Option dialer.

AdminClientInstaller—Installs the Administration Client on a system that is not running other Unified CCE components. The AdminClientInstaller is delivered on the installation media with the installer.

Administration Client Setup—Used to add, edit, or remove Administration Clients and Administration Client Instances. The Administration Client Setup is delivered on the installation media with the installer.

Enhanced Database Migration Tool (EDMT)—A wizard application that is used for all upgrades to migrate the HDS, Logger, and BA databases during the upgrade process. Back up your databases before running this tool. The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. On the other hand, errors stop the migration process and leave the database in a corrupt state. If an error occurs, restore the database from your backup, fix the error, and run the tool again.

Note If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.

You can download the EDMT from Cisco.com by clicking Cisco Enhanced Data Migration Tool Software Releases.

Note The installer, not the EDMT, upgrades the AW database for the Administration & Data Server.

User Migration Tool—A standalone Windows command-line application that is used for all upgrades that involve a change of domain. The tool imports the previously exported user accounts into the target domain during the upgrade.

You can download the User Migration tool from Cisco.com.

Regutil Tool—Used in Technology Refresh upgrades, exports the Cisco Systems, Inc. registry from the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

You can download the Regutil tool from Cisco.com.

Related Topics

Update the Java Runtime Environment (Optional), on page 57
Common Ground Upgrade Task Flow

For the Unified CCE core components, there is a general flow for redundant systems to ensure that contact center operation continues during the entire upgrade process. Sides A and B are brought down, upgraded, tested, and brought back up in a sequence that ensures continuous operation of the contact center.

For Common Ground upgrades, perform the following upgrade tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent and supervisor desktops</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Queuing and self-service components</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Infrastructure and media resource components</strong></td>
<td></td>
</tr>
<tr>
<td>Upgrade voice and data gateways.</td>
<td>Upgrade Voice and Data Gateways, on page 201</td>
</tr>
<tr>
<td><strong>Reporting server</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Unified CCE Central Controller and Administration &amp; Data Server components</strong></td>
<td></td>
</tr>
<tr>
<td>Bring down Side A Logger, and upgrade the VM to the new platform of Windows Server and SQL Server.</td>
<td>Upgrade to Windows Server 2012 R2, on page 192 Upgrade to SQL Server 2014, on page 194</td>
</tr>
<tr>
<td>Migrate Side A Logger database, and upgrade the Logger.</td>
<td>Migrate Unified CCE Logger Database and Upgrade Logger, on page 195</td>
</tr>
<tr>
<td>Bring down Side A Call Router, and upgrade the VM to new platform of Windows Server.</td>
<td>Upgrade to Windows Server 2012 R2, on page 192</td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Upgrade Side A Call Router.</td>
<td>Upgrade Unified CCE Call Router, on page 196</td>
</tr>
<tr>
<td>Upgrade the VM for the Administration &amp; Data Server connected to Side A to the new platform of Windows Server and SQL Server.</td>
<td>Upgrade to Windows Server 2012 R2, on page 192</td>
</tr>
<tr>
<td>Upgrade the Administration &amp; Data Server connected to Side A.</td>
<td>Upgrade to Windows Server 2012 R2, on page 192</td>
</tr>
<tr>
<td>Upgrade the Administration &amp; Data Server connected to Side A.</td>
<td>Upgrade to SQL Server 2014, on page 194</td>
</tr>
<tr>
<td>Bring Side A Logger and Call Router into service, bring down Side B Logger and Call Router.</td>
<td>Migrate HDS Database and Upgrade the Unified CCE Administration &amp; Data Server, on page 197</td>
</tr>
<tr>
<td>Upgrade the VM for the Side B Logger to the new platform of Windows Server and SQL Server.</td>
<td>Upgrade to Windows Server 2012 R2, on page 192</td>
</tr>
<tr>
<td>Migrate Side B Logger database and upgrade the Logger.</td>
<td>Migrate Unified CCE Logger Database and Upgrade Logger, on page 195</td>
</tr>
<tr>
<td>Upgrade the VM for the Side B Call Router to new platform of Windows Server.</td>
<td>Upgrade to Windows Server 2012 R2, on page 192</td>
</tr>
<tr>
<td>Upgrade Side B Call Router.</td>
<td>Upgrade Unified CCE Call Router, on page 196</td>
</tr>
<tr>
<td>Bring Side B Call Router into service and verify operation.</td>
<td>Verify operation of upgraded Side B Call Router and Logger, on page 203</td>
</tr>
<tr>
<td>Bring Side B Logger into service and verify operation.</td>
<td></td>
</tr>
<tr>
<td>Upgrade the VM for the Administration &amp; Data Server connected to Side B to the new platform of Windows Server and SQL Server.</td>
<td>Upgrade to Windows Server 2012 R2, on page 192</td>
</tr>
<tr>
<td>Upgrade the Administration &amp; Data Server connected to Side B.</td>
<td>Upgrade to SQL Server 2014, on page 194</td>
</tr>
<tr>
<td>Upgrade Cisco Unified Intelligence Center reporting templates.</td>
<td>Upgrade HDS Database and Upgrade the Unified CCE Administration &amp; Data Server, on page 197</td>
</tr>
<tr>
<td>Upgrade Administration Client.</td>
<td>Upgrade Unified CCE Administration Client, on page 199</td>
</tr>
<tr>
<td>Database Performance Enhancement.</td>
<td>Database Performance Enhancement, on page 206</td>
</tr>
<tr>
<td><strong>Unified CCE Peripheral Gateways and associated components</strong></td>
<td><strong>Upgrade PGs to new platform of Windows Server.</strong></td>
</tr>
<tr>
<td><strong>Upgrade PGs to new platform of Windows Server.</strong></td>
<td><strong>Upgrade to Windows Server 2012 R2, on page 192</strong></td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>Upgrade PGs.</td>
<td>Upgrade Peripheral Gateways, on page 198</td>
</tr>
<tr>
<td>Upgrade Outbound Option Dialer.</td>
<td>Upgrade Outbound Option Dialer, on page 198</td>
</tr>
</tbody>
</table>

**Desktop client components**

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
</table>

**Note** The CTI Toolkit Desktop and Cisco Agent Desktop were deprecated in Unified CCE Release 11.0(1). Do not include these desktops in new deployments. Support for these desktops will be removed in a future release.

**Call processing components**

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade (uninstall and reinstall) the JTAPI client on the Cisco Unified Communications Manager PG.</td>
<td>Upgrade Cisco JTAPI Client on the Unified Communications Manager PG, on page 205</td>
</tr>
</tbody>
</table>
### Task | See
--- | ---
**Media recording components** | 

*If you are using IP IVR for self-service and queueing, see *Getting Started with Cisco Unified IP IVR.*

### Related Topics

- Multistage Upgrades and Maintenance Windows, on page 167

### Common Ground Upgrade Tasks

The following section provides instructions about upgrading the virtual environment and the Unified CCE components. For instructions about upgrading non-Unified CCE components in a Unified CCE solution, see the links to component-specific documents in the Common Ground Upgrade Task Flow, on page 189.

### Upgrade to Windows Server 2012 R2

Microsoft supports in-place upgrade of the operating system and SQL. This topic does not provide instructions for upgrading to Microsoft Windows Server 2012 R2. For this information, see the corresponding Microsoft documentation. This topic only highlights the actions that you perform before you attempt the upgrade and after you complete the upgrade of the operating system.

---

**Important**  

---

**Before You Begin**

- Using Unified CCE Service Control, stop all Unified CCE services on the Unified CCE servers that you are upgrading, and set the startup type as **Manual**.

- If you are upgrading the Logger, ensure that you have disabled configuration changes by performing the following steps:

  1. On the A side of the CallRouter in the system that you are upgrading, set the **HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM<instance_name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance** key to 1.

  2. On the B side of the CallRouter in the system that you are upgrading, set the **HKEY_LOCAL_MACHINE\Software\Cisco Systems, Inc.\ICM<instance_name>\RouterB\Router\CurrentVersion\Configuration\Global\DBMaintenance** key to 1.
3 Verify that configuration changes are prevented. When you attempt to save a configuration change, you should see the following message: Failed to update the database. Exclusive access to the CallRouter denied because configuration changes are currently disabled in the router registry.

- If the virtual machine has SCSI Controller type as LSI Logic Parallel, change it to LSI Logic SAS. For more information, see Change the SCSI Controller Type, on page 184.

- If you did not already upgrade the VM network adapters to VMXNet3, upgrade them before upgrading the OS. see Upgrade VM Network Adapters from E1000 to VMXNet3, on page 185.

- Upgrading to Windows Server 2012 R2 may delete the persistent static routes and static network configurations (for private and public interfaces). Record your configurations before starting the upgrade process, and reconfigure it after the upgrade completes.

Note If your persistent static route uses the private interface IP address as the gateway IP, change it to use the local gateway IP.


- Ensure that the VM does not have a ghosted network adapter before the upgrade.

  During an upgrade, you can lose Static Network configuration if there is a ghosted network adapter on the VM.

  Make any ghosted network adapter visible and uninstall it from the device manager before the upgrade to Windows Server 2012 R2 Standard. see Upgrade VM Network Adapters from E1000 to VMXNet3, on page 185.

- In the vSphere Client, ensure that you have upgraded the VM hardware version to the version 9 see VM Hardware Version Upgrade, on page 186.

- Change the guest operating system to Microsoft Windows Server 2012 (64 bit). To do so, right-click the virtual machine, select Edit settings > Options > General Options and select the guest operating system as Microsoft Windows Server 2012 (64 bit) and ensure the VM is powered off during this procedure.

- Ensure that the virtual machine has enough space before the upgrade. Operating System upgrade to Windows Server 2012 requires minimum of 16-GB primary hard disk space. If the virtual machine is a Logger/Distributor machine, the upgrade to SQL Server 2014 Standard or Enterprise edition requires an extra 6 GB.

Note If you are performing the Windows upgrade on an AW-only server that does not have 16 GB, then upgrade the AW-only server using Technology Refresh.

What to Do Next
After upgrading your operating system to Windows Server 2012 R2, do the following:

- Remove the previous windows installation. see Remove Previous Windows Installation, on page 194.
Remove Previous Windows Installation

**Before You Begin**

Enable Desktop Experience under User Interfaces and Infrastructure. This step is necessary for the disk cleanup process.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click Start, search disk cleanup and then click Disk Cleanup.</td>
</tr>
<tr>
<td>2</td>
<td>In the Disk Cleanup Options dialog box, click Files from all users on this computer.</td>
</tr>
<tr>
<td>3</td>
<td>In the User Account Control dialog box, click Continue.</td>
</tr>
<tr>
<td>4</td>
<td>Click to select the previous Windows Installation check box, and then click OK.</td>
</tr>
</tbody>
</table>

Upgrade to SQL Server 2014

Microsoft supports in-place upgrade of operating system and SQL Server. After you upgrade the operating system, upgrade SQL Server.

**Note**

For information about supported editions or service packs, see the Unified CCE Solution Compatibility Matrix at http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE.

**Before You Begin**

- The upgrade to SQL Server 2014 requires a minimum of 6-GB hard disk space. Ensure that the virtual machine has the required space before you begin the upgrade.

- Ensure that the virtual machine has SQL Server 2008 R2 SP2. Ensure that your SQL Server 2008 R2 installation works properly. Set the SQL Server service to Active state during the upgrade.
• If the virtual machine has SQL Server 2008 R2 Enterprise, then upgrade to SQL Server 2014 Enterprise version only. However, if the virtual machine has SQL 2008 R2 Standard Edition, it can be upgraded to either SQL Server 2014 Standard or Enterprise Edition.

• If present, remove DB-lib registry key from the location
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSSQLServer\Client\DB-Lib
  before starting the SQL upgrade.

Procedure

Step 1
Run the SQL Server 2014 Standard or Enterprise Edition installer. Consult Microsoft documentation as needed.

Step 2
Step through the wizard. As appropriate, accept the default or choose the correct instance for your deployment. Select Rebuild on the Full-Text Search Upgrade Options page.

Step 3
After the upgrade, change the SQL Server and SQL Server Agent service accounts to Virtual accounts. To change to Virtual account:

1. Open SQL Server 2014 Configuration Manager.
2. Under SQL server services, right-click SQL Server(MSSQLSERVER), and select Properties.
3. Select This Account.
4. In the Account Name field, enter NT SERVICE\MSSQLSERVER.
6. Click OK.

Repeat the same steps for SQL Server Agent with Account Name as NT SERVICE\SQLSERVERAGENT and start the services.

Note: While you can use the Network or Local Services account instead of the Virtual account, using the Virtual account provides better security.

Note

• SQL Server Client Tools of SQL Server 2008 R2 remain on the server along with the same tools of SQL Server 2014. These tools include SQL Server Management Studio, SQL Server Profiler, the Database Engine Tuning Advisor, sqlcmd, and osql.

• SQL Server 2014 supports importing of settings from earlier versions of SQL Server Client Tools.

Migrate Unified CCE Logger Database and Upgrade Logger

To upgrade the Logger, you do the following tasks:

• Migrate the Logger database.

• Install the new software.
Setup the new Logger through the Web Setup tool.

If you use Outbound Option, you migrate the associated BaA database during this procedure.

**Before You Begin**

Before you perform this procedure, ensure that you have upgraded the VM to the new platform of Windows Server and SQL Server.

**Procedure**

1. **Step 1** Using Unified CCE Service Control, stop all Unified CCE services on the Server and change to Manual Start.
2. **Step 2** Launch the EDMT, and click Next.
3. **Step 3** Select Common Ground, and click Next.
4. **Step 4** On the warning message, click Yes if you have taken a backup of your database, and no services are currently running.
   - **Note** If you have not taken the backup of your database, click No to exit the installer.
5. **Step 5** In the Database Connection section, highlight the database that you want to upgrade, and then click Next.
6. **Step 6** Click Start Migration. A warning message is displayed asking for confirmation of the data migration.
7. **Step 7** Click Yes to confirm.
8. **Step 8** Click OK to acknowledge the message. After completion of the data migration, a warning message is displayed telling you to select a valid deployment type.
9. **Step 9** Exit the EDMT.
   - If Outbound Option is deployed, repeat the same steps to migrate the BA database.
10. **Step 10** To upgrade the Logger, launch the ICM-CCE-CCHInstaller by running setup.exe, and click Next.
11. **Step 11** (Optional) To apply any Maintenance Releases, click Browse and navigate to the Maintenance Release software. Click Next.
12. **Step 12** (Optional) Select SQL Server 2014 Security Hardening and click Next.
13. **Step 13** Click OK on any informational messages that display.
14. **Step 14** Click Install.
15. **Step 15** Reboot the server when the upgrade completes.

**Related Topics**

- Upgrade to SQL Server 2014, on page 194
- Upgrade to Windows Server 2012 R2, on page 192

**Upgrade Unified CCE Call Router**

**Before You Begin**

Before you perform this procedure, ensure that you have upgraded the virtual machine to new platform of Windows. For more information, see Upgrade to Windows Server 2012 R2, on page 192.
**Procedure**

**Step 1** Reboot the Call Router virtual machine.
**Step 2** Launch the ICM-CCE-CCHInstaller and click Next.
**Step 3** (Optional) To apply any Maintenance Releases, click Browse and navigate to the Maintenance Release software. Click Next.
**Step 4** Click OK on any informational messages that display.
**Step 5** Click Install.
**Step 6** Reboot the server when the upgrade completes.

---

**Migrate HDS Database and Upgrade the Unified CCE Administration & Data Server**

The deployment of the Administration & Database Server determines which tools to use for an upgrade:

- For an AW-only deployment, the EDMT is not required; the ICM-CCE-CCHInstaller completes the upgrade.
- For any deployment that involves an HDS database, use the EDMT to migrate the HDS database before running the installer.

**Before You Begin**

Before you perform this procedure, ensure that you have upgraded the VM to the compatible versions of Windows Server and SQL Server.

**Procedure**

**Step 1** Using Unified CCE Service Control, stop all Unified CCE services on the Server and change to Manual Start.
**Step 2** For HDS-related deployments, launch the EDMT and click Next. Select Common Ground and click Next. Review or change the information that is displayed as required and click Start Migration. Click Yes on the warning message that displays. Exit the EDMT.
**Step 3** Launch the ICM-CCE-CCHInstaller and click Next.
**Step 4** Optional: To apply any Maintenance Releases, click Browse and navigate to the Maintenance Release software. Click Next.
**Step 5** (Optional) Select SQL Server 2014 Security Hardening and click Next.
**Step 6** Click OK on any informational messages that display.
**Step 7** Click Install.
**Step 8** Reboot the server when the upgrade completes.

**Note** The time required to complete a data migration varies in a direct relationship to the database size (the larger the database size, the longer it takes to migrate) and the server hardware performance level.
Upgrade Peripheral Gateways

You can upgrade different Peripheral Gateways (PGs) within a contact center within different maintenance windows. However, upgrade all PGs that reside on the same virtual machine and their redundant PGs (Side A and then the corresponding Side B; or vice-versa) during the same maintenance window.

The following dependencies occur when upgrading the Unified Communications Manager PG:

- If your contact center uses the CTI OS component, upgrade the CTI OS server at the same time as the associated Unified Communications Manager PG.
- If your contact center uses Outbound Option, upgrade any Outbound Option Dialers that are associated with Unified Communications Manager PGs at the same time.
- When you upgrade the Unified Communications Manager application, upgrade the JTAPI client that is associated with the Unified Communications Manager PG at the same time.

Before You Begin

Before you perform this procedure, ensure that you have upgraded the virtual machine to the new platform of Windows. For more information, see Upgrade to Windows Server 2012 R2, on page 192.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch the ICM-CCE-CCHInstaller and click Next.</td>
</tr>
<tr>
<td>Step 2</td>
<td>(Optional) To apply any Maintenance Releases, click Browse and navigate to the Maintenance Release software. Click Next.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click OK on any informational messages that display.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Install.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Reboot the server when the upgrade completes.</td>
</tr>
</tbody>
</table>

Related Topics

- Upgrade to SQL Server 2014, on page 194
- Upgrade to Windows Server 2012 R2, on page 192
- Set up Peripheral Gateways, on page 47

Upgrade Outbound Option Dialer

During the upgrade, information about which contacts were called and which you need call is lost for in-process outbound campaigns. Plan the timing of the upgrade accordingly.
Procedure

**Step 1** Launch the ICM-CCE-CCHInstaller and click Next.

**Step 2** (Optional) To apply any Maintenance Releases, click Browse and navigate to the Maintenance Release software. Click Next.

**Step 3** (Optional) Select SQL Server 2014 Security Hardening and click Next.

**Step 4** Click OK on any informational messages that display.

**Step 5** Click Install.

**Step 6** Reboot the server when the upgrade completes.

**Step 7** Use Unified CCE Service Control to set all Unified CCE services to Automatic Start.

---

Upgrade Unified CCE Administration Client

Procedure

**Step 1** Launch the AdminClientInstaller and click Next.

**Step 2** (Optional) To apply any Maintenance Releases, click Browse, and navigate to the Maintenance Release software. Click Next.

**Step 3** Click OK on any informational messages that display.

**Step 4** Click Install.

**Step 5** Reboot the server when the upgrade completes.
Common Upgrade Tasks

- Upgrade Voice and Data Gateways, page 201
- Bring upgraded Side A into service, page 202
- Verify operation of upgraded Side B Call Router and Logger, page 203
- Upgrade Cisco JTAPI Client on the Unified Communications Manager PG, page 205
- Database Performance Enhancement, page 206

Upgrade Voice and Data Gateways

Perform the following procedure on each machine that hosts gateways that are used for TDM ingress, Outbound Option dialer egress, and VXML processing.

**Procedure**

**Step 1**
For VXML gateways only, perform this step. For all other gateways, proceed to the next step.

Run the `#copy tftp flash <IP Address> <filename>.bin` command to copy the flash from a remote machine to the gateway.

**Step 2**
Run the `#sh flash` command to check the version.

**Step 3**
Run the following commands in order:

a) `#conf t`
b) `#no boot system flash: <old image>`
c) `#boot system flash: <new image>`
d) `#wr`
e) `#reload`

**Step 4**
Run the `#sh version` command to verify that the new version shows in the gateway.
Bring upgraded Side A into service

After the Side A Unified CCE Logger, Call Router, and Administration & Data Server are upgraded, follow this procedure to bring Side A into service.

Procedure

**Step 1**
Use Unified CCE Service Control to stop all Unified CCE services and shut down all non-upgraded Administration & Data Servers and the Side B Call Router and Logger. Start the upgraded side.

**Step 2**
Manually start the Unified CCE services on the Side A Call Router and Logger, and the upgraded Administration & Data Server. Verify the following basic operations of the Side A Central Controller categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>• Setup logs indicate no errors or failure conditions</td>
</tr>
<tr>
<td></td>
<td>• AD domain has all users</td>
</tr>
<tr>
<td></td>
<td>• Schema upgrade is successful for all databases (no loss of data integrity or loss of data)</td>
</tr>
<tr>
<td></td>
<td>• All component services start without errors</td>
</tr>
<tr>
<td></td>
<td>• Calls are successfully processed</td>
</tr>
<tr>
<td>Call Router</td>
<td>• The Rtsvr logs indicate that the upgraded Administration &amp; Data Server has connected successfully</td>
</tr>
<tr>
<td>Logger</td>
<td>• Recovery process not required, no activity other than process start up</td>
</tr>
<tr>
<td></td>
<td>• Users are in correct domain</td>
</tr>
<tr>
<td></td>
<td>• Configuration information is passed to Call Router</td>
</tr>
<tr>
<td></td>
<td>• Replication process begins when HDS comes online</td>
</tr>
<tr>
<td>Administration &amp; Data Server</td>
<td>• The updateAW process logs indicate that the Administration &amp; Data Server is waiting for work</td>
</tr>
<tr>
<td></td>
<td>• Replication process begins with no errors</td>
</tr>
<tr>
<td>Security</td>
<td>• Specified users are able to use configuration manager</td>
</tr>
<tr>
<td>Category</td>
<td>Operation</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Script Editor</td>
<td>• Previous settings for users are present when application is opened</td>
</tr>
<tr>
<td></td>
<td>• Validate All script yields the same results that the preupgrade test yielded</td>
</tr>
<tr>
<td></td>
<td>• You can open, edit, delete, or create new scripts</td>
</tr>
<tr>
<td>ICMDBA</td>
<td>• Import/Export functionality is present</td>
</tr>
<tr>
<td></td>
<td>• Database space allocation and percent used are correct</td>
</tr>
</tbody>
</table>

During replication, data from Config_Message_Log table is replicated from Logger database to AW database. A purge mechanism is also introduced for Config_Message_Log table in AW Database. The default retention period is set to 90 days. To change the retention period, modify the following registry key:

```
Cisco Systems, Inc.\ID\<instancename>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Retention\System\ConfigMessageLog
```

**Step 3** Use Unified CCE Service Control to set the Unified CCE services to Automatic Start on each of the upgraded Unified CCE components.

**Warning** Call processing is impacted until the next three steps are completed, and therefore they must be executed at an appropriate preplanned time.

At this time, default networking should occur.

**Step 4** Use the Unified CCE Service Control to stop the services on the Side B Logger and the Side B Call Router, and all Administration & Data Servers.

**Step 5** Configure all other Unified CCE components (PGs, gateways, NAMs, multimedia components) to connect to the upgraded Side A Logger and Side A Call Router.

**Step 6** Use Unified CCE Service Control to start the services on the upgraded Side A Logger and Side A Call Router. Start the processes on the Administration & Data Server after its upgrade process completes at any point at or after this step.

**Step 7** Verify production system operation while running with the upgraded Side A Call Router and Side A Logger.

---

**Verify operation of upgraded Side B Call Router and Logger**

**Procedure**

**Step 1** Before bringing Side B into service, manually synchronize Logger B to Logger A using ICMDBA.

**Step 2** Start the Side B Call Router and Logger services.

As each node starts up, it searches for the other server components and attempts to register with them. If you completed the ICM-CCE-CCHInstaller and network testing successfully, no major errors should occur.
To verify whether a process is up, use the Diagnostic Framework Portico ListProcess option, available through the Unified CCE Tools shortcut that is created by the installer.

In order to add configuration data, the Central Controller and Administration & Data Servers must be running. The Unified CCE software loads the Unified CCE Service Control Tool on the desktop of each server and is used to control the services that are loaded on that machine.

Verify that the Unified CCE processes have no errors:

<table>
<thead>
<tr>
<th>Category</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Routers</td>
<td>• Router: Running and synchronized with peer.</td>
</tr>
<tr>
<td></td>
<td>• Rtsvr: Indicates no connectivity to Administration &amp; Data Server at this time.</td>
</tr>
<tr>
<td>Loggers</td>
<td>• Logger: Connected to its respective database and synchronized with peer. MDS is in service.</td>
</tr>
<tr>
<td></td>
<td>• Replication: No connectivity to Administration &amp; Data Server HDS at this time.</td>
</tr>
</tbody>
</table>

**Step 3** Use Unified CCE Service Control to start the Unified CCE services. Verify that the Unified CCE processes have no errors:

<table>
<thead>
<tr>
<th>Category</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Routers</td>
<td>• Router: Running and synchronized with peer.</td>
</tr>
<tr>
<td></td>
<td>• Ccagent: In service but not connected to any peripheral gateways.</td>
</tr>
<tr>
<td></td>
<td>• Rtsvr: Feed activated to Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Loggers</td>
<td>• Logger: Connected to its respective database and synchronized with peer. MDS is in service.</td>
</tr>
<tr>
<td></td>
<td>• Replication: Connected to the Administration &amp; Data Server.</td>
</tr>
<tr>
<td>Administration &amp; Data Server</td>
<td>• Updateaw: Displays &quot;Waiting for new work.&quot;</td>
</tr>
<tr>
<td></td>
<td>• Iseman: Listen thread waiting for client connection. (Exists only if Internet Script Editor is configured.)</td>
</tr>
<tr>
<td></td>
<td>• Replication: Replication and recovery client connection initialized.</td>
</tr>
</tbody>
</table>
During replication, data from Config_Message_Log table is replicated from Logger database to AW database. A purge mechanism is also introduced for Config_Message_Log table in AW Database. The default retention period is set to 90 days. To change the retention period, modify the following registry key:

```
Note: Cisco Systems, Inc.\ICM\<instancetype>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog
```

**Step 4** Validate the following settings from the system diagram for the Production Environment and make the required changes before you place the systems in production:

a) Clear event logs.
b) Remove any media from drives.
c) Ensure that all services are set to Manual Start. Services are not set to Automatic Start until after the implementation testing in the production environment.

**Step 5** Use Unified CCE Service Control to start the Unified CCE services on the new Side B Call Router and Logger. If possible, after data synchronization is complete between the Loggers, cycle the Unified CCE services on the Side A Call Router and Side A Logger and verify that Side B takes over and that the system continues to operate normally.

**Step 6** Verify overall system operation.

**Step 7** Enable configuration changes.

a) Set the following registry key to 0 on the Side A and Side B Call Routers of the system:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instancetype>\Router<A/B>\Router\CurrentVersion\Configuration\Global\DBMaintenance
```

b) Verify that configuration changes can be made.
c) Sign in to Unified CCE Administration and use the Configure Deployment tool to select the deployment type.

**Step 8** Upgrade any other Administration & Data Servers or HDSs using the steps documented in Migrate HDS Database and Upgrade Unified CCE Administration & Data Server, on page 219.

---

**Upgrade Cisco JTAPI Client on the Unified Communications Manager PG**

If you upgrade Unified Communications Manager in the contact center, also upgrade the JTAPI client that resides on the Unified Communications Manager PG. To upgrade the JTAPI client, uninstall the old version of the client and reinstall a new version. You install the JTAPI client using the Unified Communications Manager Administration application.

**Before You Begin**

You must have uninstalled the old JTAPI client from the Unified Communications Manager PG before you perform this procedure.
**Procedure**

**Step 1**  
To launch the Unified Communications Manager Administration application, enter the following URL in a web browser on the server that hosts the Unified Communications Manager: https://<Unified Communications Manager machine name>.

**Step 2**  
Enter the username and password that you created when you installed and configured Unified Communications Manager.

**Step 3**  
Select Application > Install Plug-ins.

**Step 4**  
Click the icon next to Cisco JTAPI for Windows.

**Step 5**  
Choose Run this program from its current location. Click OK.

**Step 6**  
If a Security Warning box appears, click Yes to install.

**Step 7**  
Choose Next or Continue through the remaining setup windows. Accept the default installation path.

**Step 8**  
Click Finish and reboot the system.

---

**Database Performance Enhancement**

After you perform a Common Ground or a Technology Refresh upgrade, follow the procedure listed below to enhance the performance of the database. This is a one-time process and must be run only on the Logger and AW-HDS databases during a maintenance window.

**Performance Enhancement of Logger Database**

Perform this procedure on Side A and Side B of the Logger database.

**Procedure**

**Step 1**  
Use the Unified CCE Service Control to stop the Logger service.

**Step 2**  
From the command prompt, run the RunFF.bat file which is located in the <SystemDrive>:\icm\bin directory.

**Step 3**  
Proceed with the application of fill factor to ICM databases.  
**Note:** Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes anywhere between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in <SystemDrive>\temp\<DatabaseName>_Result.txt.

**Step 4**  
Use the Unified CCE Service Control to start the Logger service.

**Troubleshooting Tips**

See the RunFF.bat/help file for more information.
Performance Enhancement of AW-HDS Database

Procedure

Step 1 Use the Unified CCE Service Control to stop the Distributor service.

Step 2 From the command prompt, run the RunFF.bat file which is located in the <SystemDrive>:\icm\bin directory.

Step 3 Proceed with the application of fill factor to ICM databases.

Note: Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in <SystemDrive>:\temp\<DatabaseName>_Result.txt.

Step 4 Use the Unified CCE Service Control to start the Distributor service.

Troubleshooting Tips
See the RunFF.bat/help file for more information.
Performance Enhancement of AW-HDS Database
Technology Refresh Upgrade

- Preupgrade Overview, page 209
- Technology Refresh Preupgrade Task Flow, page 210
- Upgrade Overview, page 212
- Technology Refresh Upgrade Task Flow, page 214
- Technology Refresh Upgrade Tasks, page 217

Preupgrade Overview

The preupgrade process ensures that your systems have the necessary software to support your contact center. These tasks prepare the way for a successful upgrade of your Cisco contact center components to the new release.

Preupgrade Tools

During the preupgrade process, use the following tools as required:

- User Migration Tool—A standalone Windows command-line application used for all upgrades that involve a change of domain. The tool exports all existing user accounts (config/setup and supervisors) in the source domain into a flat file. The file is used in the target domain during the upgrade. You can download the User Migration Tool from Cisco.com by clicking ICM User Migration Tool Software.

- Regutil Tool—Used in Technology Refresh upgrades, exports the Cisco Systems, Inc. registry from the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process. You can download the Regutil Tool from Cisco.com by clicking Contact Center Enterprise Tools.

- Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks. The ICMDBA Tool is delivered with the main installer.

- Domain Manager—Used to provision Active Directory.
The Domain Manager Tool is delivered with the main installer.

**Technology Refresh Preupgrade Task Flow**

Perform the following Technology Refresh preupgrade tasks in any order:

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain licenses</td>
<td>Cisco Product License Registration Web Site</td>
</tr>
<tr>
<td>Back up Logger, HDS, BA databases using Microsoft SQL Server Backup and Restore utility. (Backup used in case of an upgrade failure.)</td>
<td>Microsoft SQL Help</td>
</tr>
<tr>
<td>ESX Supportability</td>
<td>ESX Supportability, on page 183</td>
</tr>
<tr>
<td>Create bootable image of operating system and network configuration</td>
<td>Use your established processes</td>
</tr>
<tr>
<td>Run the following and save the results:</td>
<td>Use your established processes</td>
</tr>
<tr>
<td>ipconfig -all</td>
<td></td>
</tr>
<tr>
<td>route print -p</td>
<td></td>
</tr>
<tr>
<td>netstat -a</td>
<td></td>
</tr>
<tr>
<td>Disable configuration changes</td>
<td>Disable Configuration Changes, on page 211</td>
</tr>
<tr>
<td>Export server registry</td>
<td>Export the Server Registry, on page 211</td>
</tr>
<tr>
<td>Install Active Directory and DNS</td>
<td>Set up Active Directory, on page 12</td>
</tr>
<tr>
<td>Export Active Directory users (Optional)</td>
<td>Migrate Active Directory and DNS, on page 223</td>
</tr>
<tr>
<td>Download the Enhanced Database Migration Tool</td>
<td>Upgrade Overview, on page 186</td>
</tr>
</tbody>
</table>
### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify all stakeholders, including:</td>
<td></td>
</tr>
<tr>
<td>• Cisco Technical Assistance Center (TAC)</td>
<td></td>
</tr>
<tr>
<td>• Local Cisco Representatives</td>
<td></td>
</tr>
<tr>
<td>• Customer Operations and Emergency Management Center</td>
<td></td>
</tr>
<tr>
<td>• Third-party vendors as applicable</td>
<td></td>
</tr>
</tbody>
</table>

### Disable Configuration Changes

Perform this step on one side only. It is automatically replicated to the other side.

**Procedure**

**Step 1**

To disable configuration changes during the upgrade, set the following registry key to 1 on the Side A Call Server:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\Router A\Router\CurrentVersion\Configuration\Global\DBMaintenance
```

**Step 2**

Confirm that configuration changes are disabled by attempting to save a configuration change. When you try to save the change, a message is displayed confirming the change failure.

### Export the Server Registry

Export the Cisco registry on each source machine that is involved in a Technology Refresh upgrade. You use the exported Cisco registry to set up your Routers, Loggers, and Cisco Outbound Option dialers.

During the upgrade process, you are prompted for the path to the exported registry file location. Perform the following procedure and note the location of the resulting file for later in the upgrade process.

Each time you run the RegUtil with the export option, if a RegUtil_<hostname>.dat file exists, the utility renames that file to RegUtil_<hostname>.dat.bak<number>.

**Procedure**

**Step 1**

Open a command prompt and change the directory to the location where the RegUtil.exe resides.

**Step 2**

Run the RegUtil tool to export the Cisco Systems, Inc. registry using the following command: `RegUtil -export [target directory]`, for example, `C:\icm\bin>RegUtil -export C:\RegUtil`

The target directory must have write access. Therefore, you cannot select the install media on a DVD. The target directory is optional. If it is not specified, the tool outputs the result of the Registry export to the current directory. The output filename is of the format RegUtil_<hostname>.dat, where hostname is the name of the source machine.
Upgrade Overview

Unified CCE Redundant Central Controller Upgrade Flow

The Unified CCE central controller consists of the Logger, Router, and Administration & Data Server. When upgrading the Unified CCE portion of your contact center, the central controller is upgraded before the other Unified CCE components. While one side (Side A or B) of the redundant system is being upgraded, the other side (Side A or B) operates in stand-alone mode.

For redundant systems, the general flow for upgrading the Unified CCE central controller is as follows:

1. Upgrade the Logger, Router, and Administration & Data Server on Side A.
2. Bring Side A into service and verify the operation. Side B is brought down as Side A is coming into service.
3. Upgrade the Logger, Router, and Administration & Data Server on Side B.
4. Bring Side B into service and verify that duplexed operation begins.

Update VM Properties

Rather than recreate the VMs from the new version of the OVA, you can manually update the VM properties to match the new OVA. After you upgrade the vSphere ESXi and before you upgrade the Unified CCE components, update the properties of each VM to match the appropriate OVA, as follows:

1. Determine the version of the OVA from which you created the VM.
2. Update the properties of each VM to match the properties of the appropriate OVA. Check the Virtualization for Unified CCE DocWiki at http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE for descriptions of each OVA.
3. Stop the VM.
4. Edit the properties of the VM to match the properties from the new version of the OVA. Save your changes.
5. Restart the VM.

Caution

Be careful when you upgrade the virtual machine network adapters. Done incorrectly, this upgrade can compromise the fault tolerance of your contact center.

For version-specific information on the VM properties in an OVA, see the http://docwiki.cisco.com/wiki/Virtualization_for_Unified_CCE.

SQL Security Hardening

You can optionally apply SQL security hardening when running the installer. If your company employs custom security policies, bypass this option. Most other deployments benefit from SQL security hardening.

Upgrade Tools

During the upgrade process, use the following tools as required:
• ICM-CCE-CCHInstaller—The main Unified CCE Installer. It copies all files into relevant folders, creates the base registries, and installs needed third-party software such as JRE, Apache Tomcat, and Microsoft .NET Framework.

Note Optionally, you can update the JRE installed by the Unified CCE Installer with a later version of the JRE. See Update the Java Runtime Environment (Optional), on page 57.

You cannot run the installer remotely. Mount the installer ISO file only to a local machine.

• Cisco Unified Intelligent Contact Management Database Administration (ICMDBA) Tool—Used to create new databases, modify or delete existing databases, and perform limited SQL Server configuration tasks.

• Domain Manager—Used to provision Active Directory.

• Web Setup—Used to set up the Call Routers, Loggers, and Administration & Data Servers.

• Peripheral Gateway Setup—Used to set up PGs, the CTI server, and the Outbound Option dialer.

• AdminClientInstaller—Installs the Administration Client on a system that is not running other Unified CCE components.

The AdminClientInstaller is delivered on the installation media with the installer.

• Administration Client Setup—Used to add, edit, or remove Administration Clients and Administration Client Instances.

The Administration Client Setup is delivered on the installation media with the installer.

• Enhanced Database Migration Tool (EDMT)—A wizard application that is used for all upgrades to migrate the HDS, Logger, and BA databases during the upgrade process.

Back up your databases before running this tool. The EDMT displays status messages during the migration process, including warnings and errors. Warnings are displayed for informational purposes only and do not stop the migration. On the other hand, errors stop the migration process and leave the database in a corrupt state. If an error occurs, restore the database from your backup, fix the error, and run the tool again.

Note If you are configuring SQL services to run as Virtual account (NT SERVICE) or Network Service account (NT AUTHORITY\NETWORK SERVICE), you must run EDMT as an administrator.

You can download the EDMT from Cisco.com by clicking Cisco Enhanced Data Migration Tool Software Releases.

• User Migration Tool—A standalone Windows command-line application that is used for all upgrades that involve a change of domain. The tool imports the previously exported user accounts into the target domain during the upgrade.
You can download the User Migration tool from Cisco.com.

- Regutil Tool—Used in Technology Refresh upgrades, exports the Cisco Systems, Inc. registry from the source machine during the preupgrade process. The output of the tool is required on the destination machine when running the Unified CCE Installer during the upgrade process.

You can download the Regutil tool from Cisco.com.

Related Topics

- Update the Java Runtime Environment (Optional), on page 57
- Upgrade VM Network Adapters from E1000 to VMXNet3, on page 185

Technology Refresh Upgrade Task Flow

For the Unified CCE core components, there is a general flow for redundant systems; Sides A and B are brought down, upgraded, tested, and brought back up in sequence. That sequence ensures the operation of the contact center during the entire upgrade process.

For Technology Refresh upgrades, perform the following upgrade tasks:

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent and supervisor desktops</strong></td>
<td></td>
</tr>
<tr>
<td>Upgrade Finesse</td>
<td>*Cisco Finesse Installation and Upgrade Guide at</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Queuing and self-service components</strong></td>
<td></td>
</tr>
<tr>
<td>Upgrade Cisco Unified Customer Voice Portal*</td>
<td>*Installation and Upgrade Guide for Cisco Unified</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Infrastructure and media resource components</strong></td>
<td></td>
</tr>
<tr>
<td>Upgrade voice and data gateways</td>
<td>Upgrade Voice and Data Gateways, on page 201</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Reporting server</strong></td>
<td></td>
</tr>
<tr>
<td>Upgrade Cisco Unified Intelligence Center server</td>
<td>*Installation and Upgrade Guide for Cisco Unified Intelligence</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Unified CCE Central Controller and Administration &amp; Data Server components</strong></td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bring down Side A Logger, migrate Logger database, and upgrade Logger</td>
<td>Migrate the Logger Database and Upgrade the Logger, on page 217</td>
</tr>
<tr>
<td>Bring down Side A Call Router, and upgrade</td>
<td>Upgrade Unified CCE Call Router, on page 219</td>
</tr>
<tr>
<td>Upgrade Administration &amp; Data Server connected to Side A.</td>
<td>Migrate HDS Database and Upgrade Unified CCE Administration &amp; Data Server, on page 219</td>
</tr>
<tr>
<td>Bring Side A Logger and Call Router into service, bring down Side B Logger and Call Router</td>
<td>Bring upgraded Side A into service, on page 202</td>
</tr>
<tr>
<td>Migrate Side B Logger database and upgrade Logger</td>
<td>Migrate the Logger Database and Upgrade the Logger, on page 217</td>
</tr>
<tr>
<td>Upgrade Side B Call Router</td>
<td>Upgrade Unified CCE Call Router, on page 219</td>
</tr>
<tr>
<td>Bring Side B Call Router into service and verify operation</td>
<td>Verify operation of upgraded Side B Call Router and Logger, on page 203</td>
</tr>
<tr>
<td>Bring Side B Logger into service and verify operation.</td>
<td></td>
</tr>
<tr>
<td>Upgrade Administration &amp; Data Server connected to Side B.</td>
<td>Migrate HDS Database and Upgrade Unified CCE Administration &amp; Data Server, on page 219</td>
</tr>
<tr>
<td>Upgrade Administration Client</td>
<td>Upgrade Unified CCE Administration Client, on page 199</td>
</tr>
<tr>
<td>Database Performance Enhancement</td>
<td>Database Performance Enhancement, on page 206</td>
</tr>
<tr>
<td><strong>Unified CCE Peripheral Gateways and associated components</strong></td>
<td></td>
</tr>
<tr>
<td>Upgrade PGs</td>
<td>Upgrade Peripheral Gateways, on page 221</td>
</tr>
<tr>
<td>Upgrade Outbound Option Dialer</td>
<td>Upgrade Outbound Option Dialer, on page 222</td>
</tr>
</tbody>
</table>
### Task Flow

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
</table>

#### Desktop Client components

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>The CTI Toolkit Desktop and Cisco Agent Desktop are deprecated in Unified CCE Release 11.0(1). Do not include these desktops in new deployments. Support for these desktops will be removed in a future release.</td>
</tr>
</tbody>
</table>

#### Call Processing components

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(Install) the JTAPI client on the Cisco Unified Communications Manager PG</td>
<td>Upgrade Cisco JTAPI Client on the Unified Communications Manager PG, on page 205</td>
</tr>
</tbody>
</table>

#### Media Recording components

|---|---|

*If you are using Unified IP IVR for self-service and queueing, see Getting Started with Cisco Unified IP IVR.*

### Related Topics

Multistage Upgrades and Maintenance Windows, on page 167
Technology Refresh Upgrade Tasks

The following section provides instructions about upgrading Unified CCE components. For instructions about upgrading non-Unified CCE components in a Unified CCE solution, see the links to component-specific documents in the Technology Refresh Upgrade Task Flow, on page 214.

Migrate the Logger Database and Upgrade the Logger

To upgrade the Logger, you do the following tasks:

- Migrate the Logger database and the Outbound Option BaA database (if deployed).
- Import the Cisco registry information.
- Install the new software.
- Set up the new Logger through the Web Setup tool.

If you use Outbound Option, you migrate the associated BaA database during this procedure.

Before You Begin

Create a shared folder in any desired location. Ensure that:

- in the Properties window > Sharing tab > Advanced Sharing, the Share this folder checkbox is checked.
- in the Properties window > Security tab, the permission level is set as full control for everyone.
**Procedure**

**Step 1** Use Unified CCE Service Control to stop all Unified CCE services on the Logger.

**Step 2** Run the EDMT from the server that hosts the destination Logger and click **Next**.

**Step 3** Select **Technology Refresh** and click **Next**.

**Step 4** Under **Source Database Connection**, in the **HostName/IP Address** field, type the Source IP and click **Refresh Database List**.

**Step 5** Select the Logger Database name, and click **Next**.

**Step 6** In the Windows Share Name field, type the name of the shared folder that you created.

**Step 7** In the Windows Share Password field, type the password of the destination machine, and click **Next**.

**Step 8** Review or change the information displayed as required and click **Start Migration**.

**Step 9** Exit the EDMT.

**Step 10** If Outbound Option is deployed, to migrate the BaA database, reopen the EDMT and click **Next**.

**Step 11** Select **Technology Refresh** and click **Next**.

**Step 12** Under **Source Database Connection**, in the **HostName/IP Address** field, type the Source IP and click **Refresh Database List**.

**Step 13** Select the Outbound Database name, and click **Next**.

**Step 14** In the Windows Share Name field, type the name of the shared folder that you created.

**Step 15** In the Windows Share Password field, type the password of the destination machine, and click **Next**.

**Step 16** Review or change the information displayed as required and click **Start Migration**.

**Step 17** Exit the EDMT.

**Step 18** Launch the ICM-CCE-CCHInstaller and click **Next**.

**Step 19** Select **Technology Refresh** and click **Next**.

**Step 20** Click **Browse** and specify the path for the RegUtil file you exported from the source machine during the preupgrade process.

**Step 21** (Optional) To apply any Maintenance Releases, click **Browse** and navigate to the Maintenance Release software. Click **Next**.

**Step 22** (Optional) Select **SQL Server 2014 Security Hardening** and click **Next**.

**Step 23** Click **OK** on any informational messages that display.

**Step 24** Click **Install**.

**Step 25** Reboot the system after the upgrade completes.

**Step 26** Open the Web Setup tool from the Installer dialog box or desktop shortcut.

**Step 27** Edit the instance as necessary.

**Step 28** (Optional) In case of Cross Domain upgrade, launch Websetup, select instance and click on "Change Domain" in order to use the new domain for destination UCCE. Edit instance and you might need to change the facility or instance number if required.

**Step 29** Edit the Logger component as necessary.

If the registry now references out-of-date network interface names or IP addresses for the public and private networks for the Logger, update this information.
Step 30 (Optional) If it is a Cross Domain upgrade, use User Migration tool to export the users and OU information which you exported from the source machine during the pre-upgrade process. See User Migration Tool in Preupgrade Overview, on page 181.

Step 31 Use Unified CCE Service Control to set all Unified CCE services on the new Logger to Manual Start.

Upgrade Unified CCE Call Router

To upgrade the Call Router, you do the following tasks:

- Import the Cisco registry information.
- Install the new software.
- Set up the new Call Router using the Web Setup tool.

Procedure

Step 1 Launch the ICM-CCE-CCHInstaller and click Next.
Step 2 (Optional) To apply any Maintenance Releases, click Browse and navigate to the Maintenance Release software. Click Next.
Step 3 Select Technology Refresh and click Next.
Step 4 Specify the path for the RegUtil file you exported from the source machine during the preupgrade process.
Step 5 Click OK on any informational messages that display.
Step 6 Click Install.
Step 7 Reboot the server when the upgrade completes.
Step 8 Open the Web Setup tool from the Installer dialog box or desktop shortcut.
Step 9 Edit the instance as necessary.
   For a domain change, change the domain of the instance. Additionally, you might need to change the facility or instance number as required.
Step 10 Edit the Call Router component as necessary.
   If the registry now references out-of-date network interface names or IP addresses for the public and private networks for the router, update this information.
Step 11 Use Unified CCE Service Control to set all Unified CCE services on the new Call Router to Manual Start.

Migrate HDS Database and Upgrade Unified CCE Administration & Data Server

To upgrade the Administration & Data Server, do the following tasks:

- Migrate the HDS database (if applicable. Non-HDS configurations do not require this action.)
- Import the Cisco registry information.
• Install the new software.
• Set up the new Administration & Data Server through the Web Setup tool.

The Installer upgrades the AW database that is associated with the Administration & Data server. The EDMT does not upgrade the AW database.

Before You Begin
Create a shared folder in any desired location. Ensure that:
• in the Properties window > Sharing tab > Advanced Sharing, the Share this folder checkbox is checked.
• in the Properties window > Security tab, the permission level is set as full control for everyone.

Procedure

Step 1 Use Unified CCE Service Control to stop all Unified CCE services on the server.
Step 2 For Administration & Data Server configurations with an HDS database, open the EDMT and click Next. For non-HDS Server configurations, go to Step 10, on page 220.
Step 3 Select Technology Refresh and click Next.
Step 4 Under Source Database Connection, in the HostName\IPAddress field, type the Source IP and click Refresh Database List.
Step 5 Select the HDS Database name, and click Next.
Step 6 In the Windows Share Name field, type the name of the shared folder that you created.
Step 7 In the Windows Share Password field, type the password of the destination machine, and click Next.
Step 8 Review or change the information displayed as required, highlight the HDS database, and click Start Migration.
Step 9 Exit the EDMT.
Step 10 Launch the ICM-CCE-CCHInstaller and click Next.
Step 11 (Optional) To apply any Maintenance Releases, click Browse and navigate to the Maintenance Release software. Click Next.
Step 12 (Optional) Select SQL Server 2014 Security Hardening and click Next.
Step 13 Select Technology Refresh and click Next.
Step 14 Specify the path for the RegUtil file you exported from the source machine during the preupgrade process.
Step 15 Click OK on any informational messages that display.
Step 16 Click Install.
Step 17 Reboot the server when the upgrade completes.
Step 18 Open the Web Setup tool from the Installer dialog box or desktop shortcut.
Step 19 Edit the instance as necessary.
Step 20 (Optional) In case of Cross Domain upgrade, launch Websetup, select instance and click on "Change Domain" in order to use the new domain for destination UCCE. Edit instance and you might need to change the facility or instance number if required.
Step 21 Edit the Administration & Data Server component as necessary. If the registry now references out-of-date network interface names or IP addresses for the public and private networks for the server, update this information.
Step 22 Use Unified CCE Service Control to set all Unified CCE services on the new Administration & Data Server to Manual Start.

**Note** The time required to complete a data migration varies in a direct relationship to the database size (the larger the database size, the longer it takes to migrate) and the server hardware performance level.

---

### Upgrade Peripheral Gateways

You can upgrade different Peripheral Gateways (PGs) within a contact center at different times within different maintenance windows. However, upgrade all PGs that reside on the same virtual machine and redundant PGs (Side A and corresponding Side B) during the same maintenance window.

The following dependencies occur when upgrading the Unified Communications Manager PG:

- If your contact center uses the CTI OS component, upgrade the CTI OS server at the same time as the associated Unified Communications Manager PG.
- If your contact center uses Outbound Option, upgrade any Outbound Option Dialers associated with Unified Communications Manager PGs at the same time.
- If the Unified Communications Manager application is upgraded, upgrade the JTAPI client associated with the Unified Communications Manager PG at the same time.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Use Unified CCE Service Control to stop all Unified CCE and CTI OS (if applicable when upgrading the Unified Communications Manager PG) services on the PG server. Change the services to Manual Start.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Launch the ICM-CCE-CCHInstaller and click <strong>Next</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) To apply any Maintenance Releases, click <strong>Browse</strong> and navigate to the Maintenance Release software. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select <strong>Technology Refresh</strong> and click <strong>Next</strong>.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Specify the path for the RegUtil file you exported from the source machine during the preupgrade process. The registry information for the Unified Communications Manager PG also contains information for the CTI OS server (if applicable).</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Click <strong>OK</strong> on any informational messages that display.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Click <strong>Install</strong>.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Reboot the system after the upgrade completes.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>After reboot, open the Peripheral Gateway Setup tool from the Installer dialog box or desktop shortcut and make any necessary changes. See the &quot;Install&quot; section of this document for specific information. If the registry now references out-of-date network interface names or IP addresses for the public and private networks for the PG, update this information.</td>
</tr>
</tbody>
</table>
Upgrade Outbound Option Dialer

To upgrade the Outbound Option Dialer, import the Cisco registry information, install the new software, and set up the new Dialer using the PG Setup tool.

**Before You Begin**

You must have previously migrated the BaA database during the Side A Logger upgrade.

**Procedure**

| Step 1 | Use Unified CCE Service Control to stop all Unified CCE services on the Dialer. |
| Step 2 | Launch the ICM-CCE-CCHInstaller and click **Next**. |
| Step 3 | (Optional) To apply any Maintenance Releases, click **Browse** and navigate to the Maintenance Release software. Click **Next**. |
| Step 4 | Select **Technology Refresh** and click **Next**. |
| Step 5 | Specify the path for the RegUtil file you exported from the source machine during the preupgrade process. |
| Step 6 | Click **OK** on any informational messages that display. |
| Step 7 | Click **Install**. |
| Step 8 | Reboot the system after the upgrade completes. |
| Step 9 | Open the Peripheral Gateway Setup tool from the Installer dialog box or desktop shortcut and edit the Dialer as required. |
| Step 10 | Use Unified CCE Service Control to set all Unified CCE services to Automatic Start. |

**Related Topics**

- Migrate the Logger Database and Upgrade the Logger, on page 217

Upgrade Unified CCE Administration Client

For Technology Refresh upgrades, perform a fresh installation for the Administration Client.

**Related Topics**

- Install Unified CCE Administration Client, on page 54
Migrate Active Directory and DNS

Migrate the existing Active Directory from Windows Server 2008 R2 to a new Windows Server 2012 R2.

Preparing existing forest via the adprep command

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Insert the Windows Server 2012 DVD into the DVD drive of the Windows Server 2008 R2 AD DS and navigate to the adprep directory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Run the command <code>adprep /forestprep</code>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Run the command <code>adprep /domainprep</code>.</td>
</tr>
</tbody>
</table>

Install Active Directory on New Domain Controller

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Select Start &gt; Run, enter <code>dcpromo</code> and click OK.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>When the Active Directory Wizard opens, click Next.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Under Domain Controller Type, select Additional Domain Controller for an Existing Domain.</td>
</tr>
<tr>
<td>Step 4</td>
<td>On the Network Credentials screen, enter the domain administrator username and password.</td>
</tr>
</tbody>
</table>
The Additional Domain Controller screen should already be filled in with the FQDN (Fully Qualified Domain Name).

**Step 5** Accept the database and log location defaults.

**Step 6** Accept the shared System Volume defaults.

**Step 7** Enter the same Restore Mode Admin password that you used for the root domain controller.

**Step 8** Check **Summary Settings**. Active Directory is not configured through NETLOGON.

**Step 9** Reboot after the Active Directory installation is complete.

**Step 10** Repeat these steps for a new alternate domain controller if necessary.

---

**Configure Active Directory sites on new domain controller**

**Procedure**

Move the new domain controller to the correct sites.

**Move Flexible Single Master Operation roles**

**Procedure**

**Step 1** On the Active Directory Domain Controller that is hosting the role to be moved, open **AD Users and Computers**, and connect to the domain controller from which the role needs to be moved.

**Step 2** Right-click under the domain name and select **Operations Masters**.

**Step 3** Under the required FSMO role tab, change the Operations Master to the designated domain controller.

**Transfer Schema Master role**

**Procedure**

**Step 1** Open Command Prompt in administrative mode and type `regsvr32 schmmgmt.dll`.

**Step 2** Open Microsoft Management Console, `mmc`.

**Step 3** Click **File** then click **Add/Remove Snap-in...**.

**Step 4** From the left side, under **Available Snap-ins**, click on **Active Directory Schema**, then click **Add** and then click **OK**.

**Step 5** Right click **Active Directory Schema**, then click **Change Active Directory Domain Controller**...

**Step 6** From the listed Domain Controllers, click on the domain controller that you want to be the schema master role holder and then click **OK**.
From the listed Domain Controllers, click on the domain controller that you want to be the schema master role holder and then click on OK.

**Step 7** In the console tree, right click Active Directory Schema [DomainController.DomanName], and then click Operations Master...

**Step 8** On the Change Schema Master page, the current schema master role holder will be displayed and the targeted schema holder as well. Change, the schema master holder to the newly added Domain Controller, click Change.

**Step 9** Click Yes to confirm the role transfer.

**Step 10** The role will be transferred and a confirmation message will be displayed. Click OK.

**Step 11** Then click Close.

---

**Redefine the time source**

Because the Primary Domain Controller Emulator is moving to another Domain Controller, the time source must be redefined as either that server or an external time source.

**Procedure**

**Step 1** On the server that is currently running the Primary Domain Controller Emulator, run the following command: 
Net time /setsntp: <DNS name of time source>

**Step 2** To synchronize a member server to the time source, see the procedure available on the Microsoft Website.

---

**Assign Global Catalogs**

**Procedure**

**Step 1** Open AD Sites and Services.

**Step 2** Connect to the Domain Controller that is designated as the Global Catalog.

**Step 3** Right-click NTDS Settings, click Properties, check Global Catalog, and click OK.

**Step 4** Repeat this procedure on all servers.
Configure member servers to point to new DNS servers

Procedure

1. In the Network Settings, open the visible network connection.
2. Open TCP/IP properties.
3. Enter the new primary and alternate DNS servers.
4. Run ipconfig /flushdns from a command prompt.
5. Verify name resolution by pinging the Unified CCE servers by name.
6. Ping the Unified CCE domain by name.

Demote current domain controllers to member servers and uninstall DNS

```markdown
Important
Before demoting domain controllers, make sure that the replication process from the old domain controllers to the new domain controllers is complete. Check the directory service with the event viewer to monitor the status. In a large domain, this process could take 30 minutes or more to complete.
```

Procedure

1. Select Start > Run, enter dcpromo. When the Active Directory Wizard opens, click Next.
2. A dialog box indicating that this server is already a Domain Controller appears. Click Next to demote it to a member server.
3. You are warned and prompted as to whether or not this is the last server in the domain. Leave the box unchecked and click Next. The subsequent screens show the progress of the domain controller removal.
4. Click Next to finish.
5. Repeat this procedure for the alternate domain controller.
7. Select Add/Remove Windows Components > Networking Services.
8. Click Details.
9. Uncheck the DNS check box, then click OK.
10. Click Next.
Upgrade Active Directory and DNS

Upgrade the existing Active Directory in Windows server 2008 R2 SP1 to Windows server 2012 R2.

In-place upgrade of domain controller Windows Server 2003 to Windows Server 2012 R2 is not supported. Instead we can migrate the existing Windows Server 2003 to new Windows Server 2012 R2, see the corresponding Microsoft documentation.

Upgrade Domain Controller

Procedure

Step 1. Insert the Windows Server 2012 DVD into the DVD drive of the Windows Server 2008 R2 AD DS and navigate to the \adprep directory.
Step 2. Run `adprep /forestprep`.
Step 3. Run `adprep /domainprep`.

Assign Global Catalog

Procedure

Step 1. Open AD Sites and Services.
Step 2. Open Server objects, and connect to the Domain Controller that is designated as the Global Catalog.
Step 3. Right-click NTDS Settings, and select Properties.
Step 4. Check the Global Catalog checkbox, and click OK.
Testing

- Testing Overview, page 229
- Testing Tasks, page 229

Testing Overview

System testing is a part of the installation, upgrade, and ongoing maintenance of a Unified CCE solution. Testing requirements and processes vary from customer to customer. Therefore, specific steps for executing tests are not included in this document.

For installations, testing must ensure all aspects of contact center operation before going live.

For upgrades, at the beginning of each maintenance window, consider running preupgrade tests to establish a benchmark. The benchmark is used when you run the postupgrade tests. Postupgrade tests are necessary for each maintenance window to ensure continued contact center operation throughout the entire upgrade process, which can span multiple maintenance windows.

If you require assistance with Unified CCE solution testing, work with your Cisco representative.

Contact centers need established tests plans and processes for all aspects of contact center operation. Have the plans, tools, and processes in place to test your contact center.

Testing Tasks

Verify Upgrade to Cisco Unified Customer Voice Portal

After upgrading Unified CVP, verify the following:
Verify IOS Gateway Upgrade

After upgrading IOS gateways, verify the following:

Procedure

Step 1 At the Cisco IOS exec level, execute the following CLI commands:

- To check that the upgraded IOS target image is running:
  
  ```
  show version
  ```

- To verify that the boot system is configured to boot the correct image:
  
  ```
  show running-config
  ```

- To verify that configuration done previously is not lost:
  
  ```
  show running-config
  ```

- To verify that the ISDN connection status is at MULTIFRAME_ESTABLISHED:
  
  ```
  show isdn status
  ```

- To verify that configured interfaces are in up/up state:
  
  ```
  show ip interface brief
  ```

- To verify manually placed incoming calls:
  
  ```
  show isdn history
  ```

- To verify IP routing from branch site to a data center:

  ```
  ping or traceroute
  ```

- To verify IP routing from one branch site to another branch site:
Verifying Upgrade to Cisco IOS-Based Transcoders and Conference Bridges

After upgrading Cisco IOS-based transcoders and conference bridges, verify the following:

Procedure

Step 1 Check if the complete configuration before the upgrade still exists.
Step 2 Check if all DSPs are registered and are functioning normally.
Step 3 Check if there are no error messages in the buffer log or console.
Step 4 Check if no dump file is created in the flash memory.
Step 5 To verify that the configuration is not lost, type the "show running-config" command.
Step 6 To verify that the interfaces are in up state, type the "show ip interface brief" command.
Step 7 Make an inbound call to a Unified IP Phone through a gateway and conference the call with another Unified IP Phone, using a conference bridge in the gateway.
Step 8 Verify IOS Transcoding is working with G711 codec configure for one device while G729 codec is configured on another device.

Verifying Upgrade to Cisco Unified CCE Router and Logger

After upgrading the Cisco Unified CCE Router and Logger, verify the following:

Procedure

Step 1 Verify basic operations such as the following:
   - Setup logs indicate no errors or failure conditions (icmsetup.txt and ICMInstall.txt, located in the \Temp directory of the disk on which the application was installed).
   - All components can "ping" public and private IP addresses as applicable.
Verify Upgrade to Cisco Real Time Administration Workstation, Historical Database Server

After upgrading the Real Time AW/HDS software, verify the following:

**Procedure**

**Step 1** Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select **Administrative Tools > Event Viewer**, then expand **Windows Logs** and review the Application and System logs.

**Step 2** After Side A Central Controller components have been upgraded, verify basic operations such as the following:

- Setup logs indicate no errors or failure conditions (icmsetup.txt and ICMInstall.txt, located in the \Temp directory of the disk on which the application was installed).
- All components can “ping” public and private IP addresses as applicable.
- Schema upgrade is successful for all databases and there is no loss of data integrity or data.
• All component services start correctly without generating errors.

• All general activities such as the ability to access SQL server and to run third-party software components like VNC or PCAnywhere, etc. are not stopped by any security application.

• Rsrv, the process that provides real time data from the Router to the AW database, is connected to the primary Administrative Workstation. (Open the Configuration Manager tool on Administration & Data server. If the tool opens without any errors, the feed is active. Additionally, use the Dumplog utility to view the uaw process. The uaw trace message shows "Waiting for new work...".)

• Configuration information is passed to the router by the Logger. Replication process begins when the Historical Database Server comes online.

• Real Time Administrative Workstation indicates that it is ready.

• Replication process begins with no errors. (use the Windows Event Viewer to view Windows Event logs).

• Authorized users are able to use the Configuration Manager on the Real Time Administrative Workstation.

• Authorized users are able to log into Cisco Unified Intelligence Center and can access both public and private reports and that all previously existing reports are still available.

• Previous settings for users are still valid when any application is opened.

• The "Validate All" script yields the same results after the upgrade as prior to the upgrade.

  Note All existing scripts can be opened and edited and new scripts can be created.

• Database space allocation and % used are reported correctly. (Use the dumplog utility to view the hlgr and rcv processes on the Logger server. The trace messages display the percentage of available free space and the log space of the database at 30 second intervals. Verify this using Microsoft SQL Management Studio to view the Logger database properties.)

• Diagnostic Framework Portico can acquire logs, capture registry information, and schedule collection of logs.

• Verify that configuration changes are possible.

---

**Verify Upgrade to Peripheral Gateways**

After upgrading the peripheral gateways, verify the following:
Verify Upgrade to CTI OS Server and Outbound Option

After upgrading the Cisco Telephony Integration Object Server and Outbound Option, verify the following:

Procedure

Step 1 Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select Administrative Tools > Event Viewer, then expand Windows Logs and review the Application and System logs.

Step 2 Ensure that all Outbound Option Agent and Transfer to VRU campaigns function as expected, including all applicable dialing modes (Preview, Direct Preview, Progressive, Predictive).

Step 3 Ensure that Import Rules function as expected by importing a Contact List and Do Not Call List as applicable.

Verify Redundancy

After you upgrade both sides of all redundant components, verify the following:

Procedure

Step 1 Stop each active component.

Step 2 Ensure that the backup component assumes an active state and that the system operation switches to the backup component with no loss of functionality.
Verify Upgrade to CTI OS and Cisco Agent Desktop Agent/Desktop Clients

After upgrading the Cisco Telephony Integration Object Server (CTI OS) and CAD agent client software, verify the following:

Procedure

Step 1 Use the Windows Event Viewer on each server to check that no exceptions, errors, or unexpected events have occurred. Select Administrative Tools > Event Viewer, then expand Windows Logs and review the Application and System logs.

Step 2 Ensure that basic calls and call functionality (such as transfers, conferences, call treatment and queuing by Unified IP IVR, and so on) are working properly.

Step 3 Check that agents are still able to log in and answer calls.

Verify Upgrade to Cisco Unified Communications Manager

After upgrading Unified Communications Manager, verify the following:

Procedure

Step 1 Verify that no error messages have occurred during the upgrade process.

Step 2 Check the upgrade log file for any errors.

Step 3 Start all first node and subsequent node servers.

Step 4 Verify that there is no replication failure between the first node and subsequent node servers.

Step 5 Verify that SIP and SCCP IP Phones are registered with Unified Communications Manager.

Step 6 Ensure that the following devices are configured correctly: gatekeeper, trunks, and CTI route points.

Step 7 Ensure that the media resources (conference bridges, MTP and transcoders) are configured correctly by checking their status.

Step 8 Verify if the end users are able to connect to their CTI managers.

Step 9 Check if the license usage is correct as reported in the License Unit Report.

Step 10 Check if services on all servers in the cluster are up.

Step 11 Perform the Unified Communications Manager first node and subsequent node process verification using the following Real Time Monitoring Tool feature verification process:
   a) Verify if Multiple Route Patterns and Route Lists are configured and working properly.
   b) Verify if Extension Mobility is configured and working properly.
   c) Verify if Unified IP Phone Services are configured and working properly.
Verify Upgrade to Cisco Unified Communications Manager
Live Data CLI Commands

- Supported Character Set for Live Data Installation CLI Commands, page 237
- Live Data AW DB Access, page 238
- Live Data Cluster Configuration, page 239
- Live Data Reporting Configuration, page 240
- Live Data Services Registration, page 242

Supported Character Set for Live Data Installation CLI Commands

When working with the CLI (and not exclusively for Live Data), you can use plain alphanumeric characters [0-9] [A-Z] [a-z] and the following additional characters:

- "." (dot)
- "," (comma)
- ".!" (exclamation mark)
- ".@" (at sign)
- ".#" (number sign)
- ".$" (dollar)
- ".%" (percent)
- ".^" (caret)
- ".*" (star)
- "._" (underscore)
- ".+" (plus sign)
- ".=" (equal sign)
- ".~" (tilde)
- ".:" (colon)
Spaces are used as input separators. Most special characters carry specific meaning to the Cisco Voice Operating System (VOS) command console (for example, ",", "|", and so on). Characters above standard ASCII are mostly ignored.

Live Data AW DB Access

The Live Data AW DB access commands allow you to configure and display CCE AW DB (real-time distributor) access for the Contact Center Enterprise Live Data Product Deployment Selection. By default, the set and show commands also test the connection from Live Data to the primary or secondary AW database, check to see if the configured user has appropriate AW DB access, and report the results.

set live-data aw-access

Use this command to set the access information to the primary or secondary CCE AW. The command also automatically tests the connection from Live Data to the primary or secondary AW, checks to see if the configured user has appropriate AW DB access, and reports the results.

You can use the optional skip-test parameter if you do not want the test performed. No checking is done to see if the configured user has appropriate AW DB access, and no results are reported.

Command Syntax

set live-data aw-access {primary | secondary} addr port db user pwd [ skip-test ]

addr

Specifies the hostname or IP address of the primary or secondary CCE AW (maximum 255 characters).

port

Specifies the listening port of the database server (range 1 through 65535).

db

Specifies the database name (maximum 128 characters).

user

Specifies the login user (maximum 128 characters).

pwd

 Specifies the login password (maximum 128 characters).

skip-test

Skips the testing of the connection from Live Data to the primary or secondary AW. No checking is done to see if the configured user has appropriate AW DB access, and no results are reported. The skip-test parameter is optional.
Related Topics

Configure SQL User Account, on page 113
Configure Live Data with AW, on page 35

unset live-data aw-access

Use this command to unset the access information to the primary or secondary CCE AW DB.

Command Syntax

unset live-data aw-access {primary | secondary}

There is a single, required parameter with two possible values.

show live-data aw-access

Use this command to display the primary and secondary CCE AW DB access information and test the connection from Live Data to each AW DB, check to see if the configured user (on each node) has appropriate AW DB access, and report the results.

You can use the optional skip-test parameter if you do not want the test performed. No checking is done to see if the configured user (on each node) has appropriate AW DB access, and no results are reported.

Command Syntax

show live-data aw-access [skip-test]

Shows the configured primary and secondary CCE AW DB access information. There are no required parameters.

skip-test

Skips the testing of the connection from Live Data to the primary or secondary AW. No checking is done to see if the configured user (on each node) has appropriate AW DB access, and no results are reported. The skip-test parameter is optional.

Related Topics

Configure SQL User Account, on page 113

Live Data Cluster Configuration

Use the following commands to set, unset, or show Live Data cluster configuration information.

set live-data secondary

Use this command to register the Live Data secondary node.
**Command Syntax**

`set live-data secondary name`

`name`

Specifies the hostname or IP address of the Live Data secondary node.

**unset live-data secondary**

Use this command to unset Live Data secondary node configuration.

`unset live-data secondary`

There are no required parameters.

**show live-data secondary**

Use this command to show Live Data secondary node configuration information.

`show live-data secondary`

There are no required parameters.

**Live Data Reporting Configuration**

**set live-data reporting-interval**

Use this command to set the Live Data reporting interval in minutes. The reporting interval is the duration of time for which values are aggregated and reported for the **To Interval** fields.

**Command Syntax**

`set live-data reporting-interval reporting-interval-in-minutes`

`reporting-interval-in-minutes`

Specifies the reporting interval in minutes. The valid values are 5, 10, 15, 30, and 60 minutes.

When you set the Live Data reporting interval, use the following command to restart the publisher and then the subscriber. (Restart the inactive node and then the active node.)

**Command Syntax**

`utils system restart`
If you restart only the publisher and not the subscriber, the new reporting interval takes effect only on the publisher; likewise, if you restart the subscriber but not the publisher, only the subscriber uses the newly set reporting interval.

When the publisher and the subscriber restart, use the show live-data reporting-interval command to validate the new interval.

**Related Topics**

show live-data reporting-interval, on page 241

### show live-data reporting-interval

Use this command to show the configured and current reporting interval for both the Live Data publisher and subscriber.

**Command Syntax**

```
show live-data reporting-interval
```

### unset live-data reporting-interval

Use this command to reset the Live Data reporting interval to the default value (which is five minutes).

**Command Syntax**

```
unset live-data reporting-interval
```

When you reset the Live Data reporting interval, use the following command to restart the publisher and then the subscriber. (Restart the inactive node and then the active node.)

**Command Syntax**

```
utils system restart
```

If you restart only the publisher and not the subscriber, the reset interval takes effect only on the publisher; likewise, if you restart the subscriber but not the publisher, only the subscriber uses the reset reporting interval.

When the publisher and the subscriber restart, use the show live-data reporting-interval command to validate the new interval.

**Related Topics**

show live-data reporting-interval, on page 241
Live Data Services Registration

**set live-data cuic-datasource**

Use this command to create or update the Live Data data source in Cisco Unified Intelligence Center. You can run the command from either the Side A or Side B (not both) Live Data node; and you must run it once for each of the Cisco Unified Intelligence Center Publisher nodes. The AW Distributor and Cisco Unified Intelligence Center Publisher must be in service.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.
- Configure Live Data endpoints in the Machine Service table.

**Command Syntax**

```
set live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd
```

- **cuic-addr**
  
  Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN). This node must be in service.

- **cuic-port**
  
  Specifies the Cisco Unified Intelligence Center REST API port. Typically this port is 8444.

- **cuic-user**
  
  Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`). This user must have system configuration administrative privileges.

- **cuic-pwd**
  
  Specifies the password to use for authentication with Cisco Unified Intelligence Center.

**show live-data cuic-datasource**

Use this command to list the Live Data data source configuration in Cisco Unified Intelligence Center. You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.
- Configure Live Data endpoints in the Machine Service table.
**Command Syntax**

`show live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd`

**cuic-addr**

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN).

**cuic-port**

Specifies the Cisco Unified Intelligence Center REST API port. Typically this port is 8444.

**cuic-user**

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

**cuic-pwd**

Specifies the password to use for authentication with Cisco Unified Intelligence Center.

**unset live-data cuic-datasource**

Use this command to delete the existing Live Data data source. Ensure that there are no existing reports or report templates that reference the Live Data data source before you run the command; otherwise, the command fails.

After you run this command successfully, you can no longer generate Live Data reports.

You can use this command after you:

- Set the AW DB connection information on the same node where you want to run this command.
- Configure Live Data endpoints in the Machine Service table.

**Command Syntax**

`unset live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd`

**cuic-addr**

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN).

**cuic-port**

Specifies the Cisco Unified Intelligence Center REST API port. Typically this port is 8444.

**cuic-user**

Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify `CUIC` as the domain with the user name (for example, `CUIC\administrator`).

This user must have system configuration administrative privileges.
cuic-pwd

Specifies the password to use for authentication with Cisco Unified Intelligence Center.

**set live-data machine-services**

Use this command to set or update the Machine Service table with the latest information from Live Data services (publisher and subscriber).

**Command Syntax**

```
set live-data machine-services awdb-user awdb-pwd
```

**awdb-user**

Use the `user@domain` format to specify the AW database domain user with write-access permission. The domain is a fully qualified domain name (FQDN). The username is a user principal name. The user must be authorized to change Unified CCE configuration.

**awdb-pwd**

Specifies the AW database user password.

**show live-data machine-services**

Use this command to display Live Data entries in the Machine Services table.

**Command Syntax**

```
show live-data machine-services [ awdb-user ] [ awdb-password ]
```

**awdb-user**

Use the `user@domain` format to specify the AW database domain user with at least read-access permission.

**awdb-password**

Specifies the AW database user password.
Certificates for Live Data

- Certificates and Secure Communications, page 245
- Export Self-Signed Live Data Certificates, page 246
- Import Self-Signed Live Data Certificates, page 247
- Produce Certificate Internally, page 248
- Deploy Root Certificate for Internet Explorer, page 249
- Set Up Certificate for Internet Explorer Browser, page 250
- Set Up Certificate for Firefox Browser, page 251

Certificates and Secure Communications

If you use HTTPS for secure Finesse, Cisco Unified Intelligence Center, and Live Data server-to-server communication, you must set up security certificates. For the Finesse and Cisco Unified Intelligence Center servers to communicate with the Live Data server, you must import the Live Data certificates and Cisco Unified Intelligence Center certificates into Finesse, and the Live Data certificates into Cisco Unified Intelligence Center:

<table>
<thead>
<tr>
<th>On Server</th>
<th>Import Certificates From</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finesse</td>
<td>Live Data and Cisco Unified Intelligence Center</td>
</tr>
<tr>
<td>Live Data</td>
<td>None</td>
</tr>
<tr>
<td>Cisco Unified Intelligence Center</td>
<td>Live Data</td>
</tr>
</tbody>
</table>

You can:

- Use the self-signed certificates provided with Live Data.
When using self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

- Produce a Certification Authority (CA) certificate internally.
- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.

**Related Topics**

- Export Self-Signed Live Data Certificates, on page 246
- Import Self-Signed Live Data Certificates, on page 247
- Obtain and Upload CA Certificate for Live Data From a Third-Party Vendor
- Set up Microsoft Certificate Server for Windows Server 2012 R2, on page 248

### Obtain and Upload Third-party CA Certificate

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Live Data, Finesse, and Cisco Unified Intelligence Center servers.

To use third-party CA certificates:

- From the Live Data servers, generate and download Certificate Signing Requests (CSR) for root and application certificates.
- Obtain root and application certificates from the third party vendor.
- Upload the appropriate certificates to the Live Data, Unified Intelligence Center, and Finesse servers.


### Export Self-Signed Live Data Certificates

Live Data installation includes the generation of self-signed certificates. If you choose to work with these self-signed certificates (rather than producing your own CA certificate or obtaining a CA certificate from a third-party certificate vendor), you must first export the certificates from Live Data and Cisco Unified Intelligence Center, as described in this procedure. You must export from both Side A and Side B of the Live Data and Cisco Unified Intelligence Center servers. You must then import the certificates into Finesse, importing the Side A certificates to the Side A Finesse servers and the Side B certificates to the Side B Finesse servers.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.
**Procedure**

**Step 1** Sign in to Cisco Unified Operating System Administration on the Live Data server (http://hostname of Live Data server/cmplatform).

**Step 2** From the **Security** menu, select **Certificate Management**.

**Step 3** Click **Find**.

**Step 4** Do one of the following:
- If the tomcat-trust certificate for your server is not on the list, click **Generate New**. When the certificate generation is complete, reboot your server. Then restart this procedure.
- If the tomcat-trust certificate for your server is on the list, click the certificate to select it. (Ensure that the certificate you select includes the hostname for the server.)

**Step 5** Click **Download .pem file** and save the file to your desktop. Be sure to perform these steps for both Side A and Side B.

**Step 6** After you have downloaded the Live Data certificates, sign in to Cisco Unified Operating System Administration on the Cisco Unified Intelligence Center server (http://hostname of CUIC server/cmplatform), and repeat steps 2 to 5.

**What to Do Next**

You must now import the Live Data and Cisco Unified Intelligence Center certificates into the Finesses servers.

**Related Topics**

- Import Self-Signed Live Data Certificates, on page 247

**Import Self-Signed Live Data Certificates**

To import the certificates into the Finesses servers, use the following procedure.

**Procedure**

**Step 1** Sign in to Cisco Unified Operating System Administration on the Finesses server using the following URL: http://FQDN of Finesses server:8080/cmplatform
Step 2  From the Security menu, select Certificate Management.
Step 3  Click Upload Certificate.
Step 4  From the Certificate Name drop-down list, select tomcat-trust.
Step 5  Click Browse and browse to the location of the Live Data or Cisco Unified Intelligence Center certificate (with the .pem file extension).
Step 6  Select the file, and click Upload File.
Step 7  Repeat steps 3 to 6 for the remaining unloaded certificate.
Step 8  After you upload both certificates, restart Cisco Finesse Tomcat on the Finesse server.

What to Do Next
Be sure to perform these steps for both Side A and Side B.

Related Topics
Export Self-Signed Live Data Certificates, on page 246

Produce Certificate Internally

Set up Microsoft Certificate Server for Windows Server 2012 R2

This procedure assumes that your deployment includes a Windows Server 2012 R2 (Standard) Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows Server 2012 R2 (Standard) domain controller.

Before You Begin
Procedure

Step 1  In Windows, open the Server Manager.
Step 2  In the Quick Start window, click Add Roles and Features.
Step 3  In the Set Installation Type tab, select Role-based or feature-based installation, and then click Next.
Step 4  In the Server Selection tab, select the destination server then click Next.
Step 5  In the Server Roles tab, check the Active Directory Certificate Services box, and then click the Add Features button in the pop-up window.
Step 6  In the Features and AD CS tabs, click Next to accept default values.
Step 7  In the Role Services tab, verify that the Certification Authority box is checked, and then click Next.
Step 8  In the Confirmation tab, click Install.
Step 9  After the installation is complete, click the Configure Active Directory Certificate Service on the destination server link.
Step 10 Verify that the credentials are correct (for the domain Administrator user), and then click Next.
Step 11 In the Role Services tab, check the Certification Authority box, and then click Next.
Step 12 In the Setup Type tab, select Enterprise CA, and then click Next.
Step 13 In the CA Type tab, select Root CA, and then click Next.
Step 14 In the Private Key, Cryptography, CA Name, Validity Period, and Certificate Database tabs, click Next to accept default values.
Step 15 Review the information in the Confirmation tab, and then click Configure.

Download CA certificate

This procedure assumes that you are using the Windows Certificate Services. Perform the following steps to retrieve the root CA certificate from the certificate authority. After you retrieve the root certificate, each user must install it in the browser used to access Finesse.

Procedure

Step 1  On the Windows domain controller, run the CLI command certutil -ca.cert ca_name.cer, in which ca_name is the name of your certificate.
Step 2  Save the file. Note where you saved the file so you can retrieve it later.

Deploy Root Certificate for Internet Explorer

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's Internet Explorer. Adding the certificate automatically simplifies user requirements for configuration.
Set Up Certificate for Internet Explorer Browser

After obtaining and uploading the CA certificates, either all users must accept the certificate or the certificate must be automatically installed via group policy.

In environments where users do not log directly in to a domain or group policies are not utilized, every Internet Explorer user in the system must perform the following steps once to accept the certificate.

Procedure

Step 1 In Windows Explorer, double-click the `ca_name.cer` file (in which `ca_name` is the name of your certificate) and then click Open.
Step 2 Click Install Certificate > Next > Place all certificates in the following store.
Step 3 Click Browse and select Trusted Root Certification Authorities.
Step 4 Click OK.
Step 5 Click Next.
Step 6 Click Finish.
   A message appears that states you are about to install a certificate from a certification authority (CA).
Step 7 Click Yes.
A message appears that states the import was successful.

**Step 8** To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools > Internet Options**.

**Step 9** Click the **Content** tab.

**Step 10** Click **Certificates**.

**Step 11** Click the **Trusted Root Certification Authorities** tab.

**Step 12** Ensure that the new certificate appears in the list.

---

### Set Up Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate.

**Note** To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Firefox browser menu, select <strong>Options</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Advanced</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the <strong>Certificates</strong> tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>View Certificates</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Import</strong> and browse to the <code>ca_name.cer</code> file (in which <code>ca_name</code> is the name of your certificate).</td>
</tr>
</tbody>
</table>
Configure NAT64 for IPv6-Enabled Deployments

NAT64 allows communication between IPv6 and IPv4 networks. For IPv6-enabled deployments, you must set up NAT64 so that supervisors on an IPv6 network can access Unified CCE Administration web tools on an IPv4 network.

You can use either Stateful and Stateless NAT64. To read more about which translation type is the most appropriate for your deployment see Table 2. Comparison Between Stateless and Stateful NAT64 here: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

Note

NAT64 is NOT supported on Mtrain IOS. Ttrain is required.

For more information, see the Compatibility Matrix for Unified CCE at http://docwiki.cisco.com/wiki/Compatibility_Matrix_for_Unified_CCE.

The following example network diagram and interface configuration demonstrates Stateful NAT64 translation between an IPv6 network and an IPv4 network.
Configure DNS for IPv6

To meet the requirement that Unified CCE Administration be accessed by FQDN, a Forward lookup AAAA record for the AW must be created in DNS.

The steps in this procedure are for a Windows DNS server.

Procedure

Step 1 In Windows, navigate to Administrative Tools > DNS. This opens the DNS Manager.
Step 2 In the Forward lookup zone, navigate to your deployment's domain name.
Step 3 Right-click the domain name and select New Host (A or AAAA).
Step 4 In the New Host dialog box, enter the computer name and IP address of the AW. Click Add Host.

Determine IPv6 Translation of IPv4 Address for DNS Entry

You can determine the IPv6 address needed for the AAAA DNS record by running a ping command on any Windows machine using mixed notation. Type "ping -6" followed by your IPv6 Nat64 Prefix, two colons, and then the IPv4 address.
In the ping response, the IPv4 address is converted to the hexadecimal equivalent. Use this address in your static AAAA record.

**Note**


## Set Up IPv6 for VOS-Based Contact Center Applications

By default, only IPv4 is enabled for Unified Communications Manager, Finesse, and Unified Intelligence Center.

If you choose to enable IPv6 on these applications, you must enable it on both the publisher/primary nodes and subscriber/secondary nodes for those applications.

You can use Cisco Unified Operating System Administration or the CLI to enable IPv6.


## Set Up IPv6 Using Cisco Unified Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on the primary and secondary VOS servers.
Set Up IPv6 for VOS-Based Applications Using the CLI

To set up IPv6 using the CLI, perform the following procedure on both the primary and secondary VOS servers.

Procedure

Step 1 Access the CLI on the VOS server.
Step 2 To enable or disable IPv6, enter:

```
set network ipv6 service {enable | disable}
```

Step 3 Set the IPv6 address and prefix length:

```
set network ipv6 static_address addr mask
```

**Example:**

```
set network ipv6 static_address 2001:db8:2::a 64
```

Step 4 Set the default gateway:

```
set network ipv6 gateway addr
```

Step 5 Restart the system for the changes to take effect.

```
utils system restart
```

Step 6 To display the IPv6 settings, enter:

```
show network ipv6 settings
```