CONTENTS

PREFACE

Preface xv

Change History xv

About This Guide xviii

Audience xviii

Related Documents xviii

Obtaining Documentation and Submitting a Service Request xviii

Field Alerts and Field Notices xix

Documentation Feedback xix

Conventions xix

CHAPTER 1

Preparation 1

Scenarios 1

Installation Scenario 1

Upgrade Scenarios 1

Common Ground Upgrades 2

Technology Refresh Upgrades 2

System Requirements 3

Platform Requirements 3

Network Requirements 4

Transport Layer Security Version 1.2 Required 4

Software License Requirements 4

Virtualization Requirements 6

ESXi Supportability 7

Compatibility Requirements 7

CHAPTER 2

Installation Overview 9
Validate Network Adapter Settings and Power On 33
Configure Network Cards 34
Configure Private Ethernet Card 34
Configure Visible Ethernet Card 34
Install Unified CCE 11.6(1) Software 35
Set up Organizational Units 36
   Add a Domain 36
   Add Organizational Units 36
   Add Users to Security Groups 37
Set Up Unified CCE Central Controller Components 37
   Add Unified CCE Instance 37
Create Component Databases 38
Add Components to Unified CCE Instance 40
   Add Logger Component to Instance 40
   Add Router Component to Instance 42
   Add Administration & Data Server Component to Instance 43
Set up Peripheral Gateways 45
   Configure Peripheral Gateways in PG Explorer 45
   Add Peripherals to Peripheral Gateways 46
   Configure Peripheral Gateway Setup 49
Install JTAPI Client on Unified Communications Manager PG 51
Set up CTI Server 52
   Add CTI Server Component 52
   Set CTI Server Properties 52
   Set CTI Server Component Properties 53
   Set CTI Server Network Interface Properties 53
   Complete CTI Server Setup 53
Install Unified CCE Administration Client 54
   Install Administration Client 54
   Set up Administration Client 54
Install Unified CCE Language Pack 55
Update the Java Runtime Environment (Optional) 55
Upgrade Tomcat Utility 56
Upgrade Tomcat 56
Silent installation 57

Silent Installation Prerequisites for Unified CCE Release 11.0(x) 57
Perform a Silent Installation for Unified CCE Release 11.0(x) 58
Silent Installation Prerequisites for Unified CCE Release 11.6(x) 58
Perform a silent installation for Unified CCE Release 11.6(x) 58

Cisco Finesse Server Installation 59

Installation Task Flow 59
Install Finesse on Primary Node 60
Configure Contact Center Enterprise CTI Server Settings 63
Configure Contact Center Enterprise Administration and Data Server settings 64
Configure Cluster Settings 65
Restart Cisco Finesse Tomcat 65
Install Finesse on Secondary Node 65

Upgrade VMware Tools 68
Check Replication Status 69

Live Data Standalone Installation 69

Set Deployment Type in Unified CCE Administration Configuration 69
Install Publishers/Primary Nodes of VOS-Based Contact Center Applications 70
Set Live Data Secondary Node 71
Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications 72
Install VMware Tools 73
Configure Live Data with AW 73
Configure Live Data Machine Services 75
Configure Live Data for Unified Intelligence Center Data Sources 75
Restart Live Data 76
Set Up Certificates for Live Data 76
Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS) 76

Set Deployment Type 77
Install Publisher/Primary Nodes of Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS) 77
Install Subscribers/Secondary Nodes of Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS) 79
Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory 80
Install VMware Tools 81
Configure Live Data with AW 81
Configure Live Data Unified Intelligence Center Data Sources 82
Restart Live Data 83

CHAPTER 5

Initial Configuration 85

Initial Configuration Overview 85
Initial Configuration Task Flow 85
Initial Configuration Tasks 86

Configure Cisco Unified Contact Center Enterprise 86
  Access Configuration Manager tool 86
  Configure Media Routing Domain 87
  Configure Trunk Groups 87
  Configure Network VRU Bank 89
  Configure services 89
  Configure dialed numbers 91
  Configure call types 92
  Configure Variables 93
  Configure Users 97
  Configure Network VRUs 103
  Configure scripts 104
  Configure Agent Targeting Rules 107
  Configure translation routes 108
  Configure Skill Groups or Precision Routing 110
  Configure Precision Routing 112
  Configure routes 118
  Perform Bulk Configuration 119

Configure Cisco Unified Intelligence Center 124
  Acquire License 124
  Sign In to Administration Console 125
  Upload License 125
  Configure SQL User Account 126
  Configure Data Sources 127
  Download Report Bundles 129
  Import Report Bundles 130
Configure Unified Intelligence Center Administration 130
Configure Cisco Unified Customer Voice Portal 131
  Configure Unified CVP Server 131
  Configure Unified CVP Reporting Server 133
  Configure Unified CVP Operations Console 135
Configure Cisco Unified Communications Manager 143
  Set Up Device Pool 143
  Set Up Unified Communications Manager Groups 143
  Set Up CTI Route Point 143
  Set Up Trunk 144
  Set Up Application User 144
  Set Up SIP Options 145
  Set Up Route Pattern 145
  Set Up Conference Bridge 146
  Set Up Media Termination Point 146
  Set Up Transcoder 146
  Set Up Media Resource Group 146
  Set Up and Associate Media Resource Group List 147
  Set Up Enterprise Parameters 148
  Configure Mobile Agent 148
  Configure Local Trunk 149
  Configure Outbound Dialer 150
  Configure A-Law Codec 150
  Configure Support for Multiline Agent Control 151
  Configure Caller-Specific Music on Hold 151
Configure Cisco Finesse 153
  Configure Contact Center Enterprise CTI Server Settings 153
  Configure Contact Center Enterprise Administration & Data Server Settings 154
  Configure Cluster Settings 155
  Restart Cisco Finesse Tomcat 155
  Check Replication Status 155
  Ensure Agents Have Passwords 156
  Ensure Logout Non-Activity Time for Agents is Configured 156
  Browser Settings for Internet Explorer 157
CHAPTER 10  Upgrade from a Standalone Deployment to a Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS) 229

Upgrade from a Standalone to a Co-resident Deployment 229
Set Deployment Type in Unified CCE Administration Configuration 229
Install and Upgrade COP File 230
Install Publisher/Primary Nodes of VOS-Based Contact Center Applications 230
Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications 232
Set Up the System Inventory 234
Install Vmware Tools 234
Configure Live Data with AW 234
Configure Live Data Unified Intelligence Center Data Sources 235
Restart Live Data 236

CHAPTER 11  Uninstall Unified CCE Release 11.6(1) 237

Uninstall Methods 237
Temporary Uninstallation 237
Permanent Uninstallation 238
  Rollback Caveats 238
  Revert Tomcat 239
Uninstall Unified CCE Release 11.6(1) 240
Uninstallation of base CCE 11.0(1) 241

CHAPTER 12  Testing 243

Testing Overview 243
Testing Tasks 243
  Verify Upgrade to Cisco Unified Customer Voice Portal 243
  Verify IOS Gateway Upgrade 244
  Verify Upgrade to Cisco IOS-Based Transcoders and Conference Bridges 245
  Verify Upgrade to Cisco Unified CCE Router and Logger 245
  Verify Upgrade to Cisco Real Time Administration Workstation, Historical Database Server 246
  Verify Upgrade to Peripheral Gateways 247
  Verify Redundancy 247
  Verify Upgrade to Cisco Unified Communications Manager 248
APPENDIX A

CLI Commands 249

LiveData CLI Commands 249
  Supported Character Set for Live Data Installation CLI Commands 249
Privilege Levels for Live Data Commands 250
LiveData AW DB Access 250
  set live-data aw-access 250
  unset live-data aw-access 251
  show live-data aw-access 251
LiveData Cluster Configuration 251
  set live-data secondary 251
  unset live-data secondary 252
  show live-data secondary 252
LiveData Reporting Configuration 252
  set live-data reporting-interval 252
  show live-data reporting-interval 252
  unset live-data reporting-interval 253
LiveData Services Registration 253
  set live-data cuic-datasource 253
  show live-data cuic-datasource 254
  unset live-data cuic-datasource 254
  set live-data machine-services 255
  show live-data machine-services 255

Transport Layer Security CLI Commands 255
  TLS Server Minimum Version 256
    set tls server min-version 256
    show tls server min-version 256
  TLS Client Minimum Version 256
    set tls client min-version 256
    show tls server min-version 256

APPENDIX B

Certificates for Live Data Standalone 257
  Certificates and Secure Communications 257
  Obtain and Upload Third-party CA Certificate 258
Export Self-Signed Live Data Certificates 258
Import Self-Signed Live Data Certificates 259
Produce Certificate Internally 260
  Set up Microsoft Certificate Server for Windows Server 2012 R2 260
  Download CA certificate 260
Deploy Root Certificate for Internet Explorer 261
Set Up CA Certificate for Internet Explorer Browser 261
Set Up CA Certificate for Firefox Browser 262

APPENDIX C  Certificate for Live Data Corepresent 265
Add Self-Signed Certificates for Live Data 265
Obtain and Upload CA Certificate for Live Data from a Third Party Vendor 266
Produce Certificate Internally 266
  Set up Microsoft Certificate Server for Windows 2008 R2 266
  Set up Microsoft Certificate Server for Windows Server 2012 R2 267
  Download CA certificate 268
Deploy Root Certificate for Internet Explorer 268
Set Up CA Certificate for Internet Explorer Browser 269
Set Up CA Certificate for Firefox Browser 269

APPENDIX D  Migrate from Co-resident Deployment to Standalone Deployment 271
Upgrade from Co-resident to Standalone Deployments 271
  Set up the System Inventory for Standalone Deployment 272

APPENDIX E  IPv6 Configuration 273
Configure NAT64 for IPv6-Enabled Deployment 273
  Configure DNS for IPv6 274
    Determine IPv6 Translation of IPv4 Address for DNS Entry 274
Set Up IPv6 for VOS-Based Contact Center Applications 275
  Set Up IPv6 Using Cisco Unified Operating System Administration 275
Set Up IPv6 for VOS-Based Applications Using the CLI 276
Preface

• Change History, on page xv
• About This Guide, on page xviii
• Audience, on page xviii
• Related Documents, on page xviii
• Obtaining Documentation and Submitting a Service Request, on page xviii
• Field Alerts and Field Notices, on page xix
• Documentation Feedback, on page xix
• Conventions, on page xix

Change History

This table lists changes made to this guide. Most recent changes appear at the top:

<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added RAID configuration for C240 M5SX servers</td>
<td>Configure RAID for C240 M5SX</td>
<td>June 2018</td>
</tr>
<tr>
<td>Added support for C240 M5SX servers.</td>
<td>Create a Virtual Machine from the OVA</td>
<td>June 2018</td>
</tr>
<tr>
<td>Added notes on fresh install of Standalone CUIC when a higher configuration is required.</td>
<td>Standalone Deployment</td>
<td>February 2018</td>
</tr>
<tr>
<td>Added details for installing COP files.</td>
<td>Install and Upgrade COP File</td>
<td>September 2017</td>
</tr>
<tr>
<td>Change</td>
<td>See</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Initial Release of Document for Release 11.6(1)</strong></td>
<td></td>
<td>August 2017</td>
</tr>
<tr>
<td>Added details related to Outbound Option high availability.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Added details on installation of .NET Framework prior to Unified CCE 11.6.</td>
<td>Preinstallation &gt; Install .NET Framework 4.5.2</td>
<td></td>
</tr>
<tr>
<td>Added TLS minimum version CLI commands</td>
<td>Appendix A, CLI Commands</td>
<td></td>
</tr>
<tr>
<td>Added another stage for Identity Service IdS Server(IdS) /Single Sign-On(SSO) and included the upgrade scenario in the note added. Updated the workflow accordingly.</td>
<td>Multistage Upgrades and Maintenance Windows&lt;br&gt; Unified CCE Contact Center Upgrade Flowcharts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Add Peripherals to Peripheral Gateways&lt;br&gt; Common Ground Upgrade&lt;br&gt; Installation Task Flow&lt;br&gt; Uninstall Unified CCE Release 11.6(1)&lt;br&gt; Verify Upgrade to Cisco Unified CCE Router and Logger&lt;br&gt; Verify Upgrade to Cisco Real Time Administration Workstation, Historical Database Server</td>
<td></td>
</tr>
<tr>
<td>Change</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Updated the step for configuring Agent Desk Settings before creating CUCM PIM. Also included a reference to Assign Agent Desk Settings. Similarly, updated the step for VRU PG, added a note and included a reference for Configure Network VRUs in the same section. Added the topic Enable Configuration changes in Common Ground Upgrade. Upgraded version (applicable for 11.6) and updated Maintenance Release with Minor Release. Removed references for Install Remote Silent Monitor and E-mail and Web Interaction since it is not more supported for 11.6. Included various scenario If you have set the newly introduced deployment as 2000 Agents Rogger and switch to different deployment which is supported in previous version of CCE Release 11.x, before attempting permanent uninstall. Updated Setup logs that indicates no errors or failure conditions. Updated the information for blocking uninstall with UCCE 2000 Agents Rogger deployment. The update is applicable when the deployment is set as UCCE: 2000 Agents Rogger, the user needs to switch to different deployment which is supported in previous version of CCE Release 11.x, before attempting permanent uninstall. Added a note in Unified CCE Release 11.6(1) Upgrade Overview, to state that CCE 11.6 applies the use of TLS 1.2 in the entire solution and upgrade to SQL Server 2014 SP2 is a prerequisite before upgrading to 11.6(1). Added a note in Upgrade to Unified CCE Release 11.6(1) section to explain the values for Major, CCMMinor, AWMMinor that are used in the backup folder name, are derived from the 11.0 or 11.5 schema version of the system being upgraded. Updated Upgrade tools section and added that the User Migration Tool (UMT) cannot be used for migrating SSO enabled users. A note was added stating the possibility of encountering locked DLL’s preventing patch installation / uninstallation, if Windows Event Viewer is left open.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Change</th>
</tr>
</thead>
</table>

---

Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, Release 11.6(1)
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.

Related Documents

<table>
<thead>
<tr>
<th>Subject</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design considerations and guidelines for deploying a Unified CCE solution, including its various components and subsystems.</td>
<td>Design Guide</td>
</tr>
<tr>
<td>System diagrams, staging steps and sample test cases for supported models of Unified CCE.</td>
<td>Staging Guide</td>
</tr>
<tr>
<td>Pre-installation requirements and issues to address when you prepare for a Unified CCE installation.</td>
<td>Preinstallation and Planning</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the . RSS feeds are a free service.
Field Alerts and Field Notices

Cisco can modify its products or determine key processes to be important. These changes 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.

Sign in www.cisco.com and then access the tool at https://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>
<tbody>
<tr>
<td><strong>boldface</strong> font</td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</td>
</tr>
<tr>
<td></td>
<td>• Choose <strong>Edit &gt; Find</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term. Example: A skill group is a collection of agents who share similar skills.</td>
</tr>
<tr>
<td></td>
<td>• A syntax value that the user must replace. Example: IF (condition, true-value, false-value)</td>
</tr>
<tr>
<td></td>
<td>• A book title. Example: See the <em>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</em>.</td>
</tr>
<tr>
<td><strong>window</strong> font</td>
<td>Window font, such as Courier, is used for the following:</td>
</tr>
<tr>
<td></td>
<td>• Text as it appears in code or that the window displays. Example:</td>
</tr>
<tr>
<td></td>
<td>&lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td><strong>&lt; &gt;</strong></td>
<td>Angle brackets are used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• For arguments where the context does not allow italic, such as ASCII output.</td>
</tr>
<tr>
<td></td>
<td>• A character string that the user enters but that does not appear on the window such as a password.</td>
</tr>
</tbody>
</table>
Preparation

- Scenarios, on page 1
- System Requirements, on page 3

Scenarios

Cisco Unified Contact Center Enterprise (Unified CCE) is supported only in a virtualized environment.

Installation Scenario

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.

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

You can use the OVA template to deploy the VMs before beginning with the installation of CCE components.

The Unified CCE 11.6(1) installer is available as an add-on release to Unified CCE 11.0(x). Therefore, complete the installation of the base Unified CCE 11.0(1) before applying Unified CCE 11.6(1). Unified CCE 11.6(1) can be installed on 11.5(x) as well.

For more information about the complete procedure, see the Installation Task Flow, on page 31.

Upgrade Scenarios

Upgrading to Unified CCE Release 11.6(1) from Unified CCE Release 11.x, is the same as upgrading or applying any other maintenance release. However, the Unified CCE 11.6(1) minor release contains an updated database schema. Before the upgrade begins, the installer takes a backup of the configuration data from the logger database of the existing Unified CCE 11.x configuration.

You can upgrade from Unified CCE Release 10.0(x)\(^1\) and 10.5(x) to Release 11.x by using one of the two methods:

- The Common Ground method is an in-place upgrade performed on your existing virtual machine which involves upgrading the Unified CCE and all other associated software hosted on it. 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. You can also bypass the Windows Server operating system and SQL Server upgrade process, as would be required when upgrading from Unified CCE Release 10.0(x) and Release 10.5(x) to Unified CCE Release 11.0(x).

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.

Upgrade to Unified CCE Release 11.6(1) by either of the methods is possible by employing an in-line upgrade (the process of specifying Release 11.6(1) installer location, while running the Release 11.0(1) base installer). The system after upgrading to Release 11.0(1) and restarting, commences upgrading to Release 11.6(1).

1 Note: The upgrade from 10.0(x) to 11.6(1) is specific to Unified CCE components (for example, Router, PG, and so on).

Common Ground Upgrades


The common ground upgrade method consists of the following tasks:

• In-place upgrade of the operating system to Windows Server 2012 R2
• SQL server upgrade (for components such as Logger and Distributor)
• Database schema migration using the Enhanced Database Migration Tool (EDMT)
• Upgrade the Unified CCE software


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 because the operating system and SQL Server upgrade steps can be by-passed.

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.

For more information, see these documents:


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>
<tbody>
<tr>
<td></td>
<td>• VMware vCenter (Optional)</td>
<td></td>
</tr>
<tr>
<td>UCS B- or C-series (Specs-based):</td>
<td>• VMware vCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VMware vSphere ESXi</td>
<td></td>
</tr>
<tr>
<td>Third-party (Specs-based):</td>
<td>• VMware vCenter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• VMware vSphere ESXi</td>
<td></td>
</tr>
</tbody>
</table>

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


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</td>
<td>One server license for each of the voice applications.</td>
</tr>
<tr>
<td>Enterprise</td>
<td>One agent license for each concurrent user with different feature tiers.</td>
</tr>
<tr>
<td>Cisco Unified Communications</td>
<td>One license for each Cisco Unified Communications Manager node, plus device licenses</td>
</tr>
<tr>
<td>Manager</td>
<td>for connected devices.</td>
</tr>
</tbody>
</table>
### Components and License Requirements

<table>
<thead>
<tr>
<th>Components</th>
<th>License requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Unified Customer Voice Portal (CVP)</td>
<td>One 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>
<tr>
<td>Cisco Finesse or Cisco CTI OS</td>
<td>Cisco 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. Cisco CTI Object Server (CTI OS): User licenses included with selected tiers of Cisco Unified Contact Center Enterprise user licenses.</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>
</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>Microsoft Windows Client Operating System</td>
<td>For Administration Client applications</td>
</tr>
</tbody>
</table>

**Preparation**

Software License Requirements
### Software

<table>
<thead>
<tr>
<th>Antivirus</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Symantec Endpoint Protection</td>
<td>For all applications that run on the Windows platform</td>
</tr>
<tr>
<td>• Trend Micro Office Scan</td>
<td></td>
</tr>
<tr>
<td>• McAfee VirusScan Enterprise</td>
<td></td>
</tr>
</tbody>
</table>

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.

## 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.

  __Note__

  Ensure that there is sufficient hard disk space to support the new release.


**Related Topics**

- Install VMware Tools, on page 23
ESXi Supportability


As part of the Common Ground upgrade process, if there are no available overlapping supported ESXi versions, upgrade the UCCE software first if a back-out of the upgrade is required.

If the upgrade is successful and working, you can then proceed to upgrade ESXi to a supported version for final testing and restoring production operation.

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>
</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. |
| Windows OS and SNMP  
  • SNMP Service  
  • SNMP MI Provider | See the following:  
<table>
<thead>
<tr>
<th>For this compatibility information</th>
<th>See</th>
</tr>
</thead>
</table>
CHAPTER 2

Installation Overview

• Installation Tools, on page 9
• Uninstallation, on page 10

Installation Tools

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

• ICM-CCE-Installer—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 55.

Do not run the installer remotely. Download the Installer to a local machine for installation.

• 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-Installer.

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

Related Topics

Update the Java Runtime Environment (Optional), on page 55
Uninstallation

Unified CCE supports the uninstall option from the Programs and Features window in the Windows Control Panel. This option removes the patches, base version files, and the related registry. The specific option also removes Unified CCE component software installed by the ICM-CCE-Installer.

However, it does not remove the following:

- Java Runtime Environment
- Unified CCE databases

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

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

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 integratingUnified 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 11</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 21</td>
</tr>
</tbody>
</table>

Preinstallation Tasks

Set up Active Directory

Ensure that you have a completed plan for your domain structure and Active Directory implementation before you set up your network. For more information, see the Staging Guide for Cisco Unified ICM/Contact Center Enterprise at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.
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 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

Step 1 Choose Start > Run.
Step 2 Type cmd.
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

Step 1 Choose Start > Run.
Step 2 Type cmd.
Step 3 Press Enter.
A command console opens.

Step 4 At the prompt, enter repadmin.exe /showrepl * /csv >showrepl.csv.

Step 5 Open Excel and choose File > Open.
Note Depending on your version of Excel, the menu cascades may be slightly different.

**Step 6** In the “Files of type” section, click **Text Files (*.prn;*.txt;*.csv)**.

**Step 7** In the “Look in” section, navigate to `showrepl.csv`, then click **Open**.

**Step 8** In the Excel spreadsheet, right-click the column heading for `showrepl_COLUMNS` (column A), then click **Hide**.

**Step 9** In the Excel spreadsheet, right-click the column heading for `Transport Type`, then click **Hide**.

**Step 10** Select the row just under the column headings, then choose **Windows > Freeze Pane**.

**Step 11** Click the upper-left corner of the spreadsheet to highlight the entire spreadsheet. Choose **Data > Filter > AutoFilter**.

**Step 12** In the heading of the Last Success column, click the **down arrow**, then click **Sort Ascending**.

**Step 13** 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.

**Step 14** 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.

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)

**Step 15** Use AutoFilter in Excel to view the replication health for the following:

- Working domain controllers only
- Failing domain controllers only
- Domain controllers that are the least, or most recent

You can observe the replication partners that replicate successfully.

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

**Step 17** Rerun `repmadmin.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 FSMO 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

Note

If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs in order to work properly.

Perform the following procedure to 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 at [https://www.vmware.com/support/pubs/](https://www.vmware.com/support/pubs/).

For more information, see [Virtualization for Unified Contact Center Enterprise](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_com/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html).

### Configure RAID for C240 M4SX

The disk array configuration for the C240 M4SX is already set up to match what is required for Unified CCE. Verify the settings as follows.

**Procedure**

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 5 (Physical Disks) * 4 (Virtual Drives/Datastores)
- Stripe Size: 128KB
Configure RAID for C240 M5SX

The disk array configuration for the C240 M5SX is already set up to match what is required for Packaged CCE. Verify the settings as follows:

Procedure

Using Cisco Integrated Management Controller, check that the following settings are configured correctly:

- Virtual Drive Info: RAID 5 with 6 (Physical Disks) * 4 (Virtual Drives/Datastores)
- Stripe Size: 128KB
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for C240 M5SX in Configure RAID with GUI (UCS C-Series M5 Servers) section, see Cisco Collaboration on Virtual Servers Guide at:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/virtual/CHCS_BK_C7C7ED05_00_cisco-collaboration-on-virtual-servers.html

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

Step 1

Go to the Unified CCE Download Software page on Cisco.com.

Step 2

Click Download 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.
Create a Virtual Machine from the OVA

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

**Note**

ECE requires a second virtual hard drive on its VM. The OVA creates one virtual hard drive. Create a second hard drive of an appropriate size for your solution requirements.

**Procedure**

**Step 1** Select the Host in the vSphere client.

**Step 2** Choose **File > Deploy OVF Template**.

**Step 3** Browse to the location on your local drive where you stored the OVA. Click **Open** to select the file. Click **Next**.

**Step 4** Click **Next** at the **OVF Template Details** page.

**Step 5** Enter the virtual machine name. It cannot contain spaces or special characters. Enter a maximum of 32 characters. Click **Next**.

**Step 6** On the **Name and Location** page, enter a name of your choice in the **Name** field. Click **Next**.

**Important** After the VM is created, you cannot rename it.

**Step 7** On the **Deployment Configuration** page, select the applicable configuration from the drop-down list. Click **Next**.

**Step 8** Choose a data store on which to deploy the new virtual machine. Click **Next**.

For each datastore, the following tables describe the RAID group, the ESXi Host, and the virtual machines for the C240 M4SX and the C240 M5SX servers.

### RAID configuration for the C240 M4SX and C240 M5SX

<table>
<thead>
<tr>
<th>RAID Group</th>
<th>VM Datastore</th>
<th>ESXi Host</th>
<th>Virtual Machines</th>
</tr>
</thead>
</table>
| VD0        | datastore 1  | A         | ESXi operating system  
Unified CCE Logger, Side A  
Unified Communications Manager Publisher  
Cisco Finesse Primary |
| VD1        | datastore 2  | A         | Unified CCE AW-HDS-DDS, Side A |
| VD2        | datastore 3  | A         | Unified Communications Manager Subscriber 1  
Unified CVP OAMP Server  
Unified CVP Server, Side A |
<table>
<thead>
<tr>
<th>RAID Group</th>
<th>VM Datastore</th>
<th>ESXi Host</th>
<th>Virtual Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>VD3</td>
<td>datastore 4</td>
<td>A</td>
<td>Unified Intelligence Center Server Publisher&lt;br&gt;Unified CCE PG, Side A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESXi operating system&lt;br&gt;Unified CCE Logger, Side B&lt;br&gt;Unified Communications Manager Subscriber 2&lt;br&gt;Cisco Finesse Secondary</td>
</tr>
<tr>
<td>VD0</td>
<td>datastore 1</td>
<td>B</td>
<td>Unified CCE AW-HDS-DDS, Side B</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unified Customer Voice Portal Reporting Server (optional)&lt;br&gt;Unified CVP Server, Side B</td>
</tr>
<tr>
<td>VD1</td>
<td>datastore 2</td>
<td>B</td>
<td>Unified CCE AW-HDS-DDS, Side B</td>
</tr>
<tr>
<td>VD2</td>
<td>datastore 3</td>
<td>B</td>
<td>Unified Intelligence Center Server Subscriber&lt;br&gt;Unified CCE PG, Side B&lt;br&gt;Enterprise Chat and Email Server (optional)</td>
</tr>
<tr>
<td>VD3</td>
<td>datastore 4</td>
<td>B</td>
<td>Unified Intelligence Center Server Subscriber&lt;br&gt;Unified CCE PG, Side B&lt;br&gt;Enterprise Chat and Email Server (optional)</td>
</tr>
</tbody>
</table>

**Note** Some deployments require two datastores.

**Step 9**
On the **Disk Format** page, choose **Thick provisioned Eager Zeroed format** for the virtual disk format. Click **Next**.

*Note* **Thick provisioned Lazy Zero** is also supported, but **Thin provisioned** is not supported.

**Step 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.

**Step 11**
Click **Finish**.

**Step 12**
At the Successfully Completed message, click **Close**.

Create a Second Hard Drive

After deploying the OVA files, the second hard drive is no longer automatically created for all deployments except for Cisco Packaged CCE deployment. To create a second hard drive:

**Procedure**

**Step 1** Right-click the virtual machine and click **Edit Settings**.

**Step 2** In the **Hardware** tab, select the hard disk to highlight it, and then click **Add**.

The **Add hardware** window appears.

**Step 3** In the Choose the type of device you wish to add section, select **Hard Disk**, and then click **Next**.

**Step 4** Select the **Create a new virtual disk** option, and then click **Next**.

**Step 5** In the Capacity section, use the **Disk Size** field to assign the desired memory, and then click **Next**.

**Note** Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. After deployment, add the default disk profile to each Virtual machine by type, as listed in the table:

<table>
<thead>
<tr>
<th>Virtual Machine Template</th>
<th>Default Second Disk Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logger</td>
<td>500 GB</td>
</tr>
<tr>
<td>Rogger</td>
<td>150 GB</td>
</tr>
<tr>
<td>AW-HDS-DDS</td>
<td>500 GB</td>
</tr>
<tr>
<td>AW-HDS</td>
<td>500 GB</td>
</tr>
<tr>
<td>HDS-DDS</td>
<td>500 GB</td>
</tr>
</tbody>
</table>

You can customize the SQL database disk space to meet data retention requirements, as calculated by the Database Estimator tool.

**Step 6** In the Advanced Options section, retain the default options and then click **Next**.

**Step 7** In the Ready to Complete section, click **Finish** to create the hard disk.

**Step 8** Click **OK** to confirm the changes.

The Recent Tasks window at the bottom of the screen displays the progress.

---

**Mount 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 file and click **OK**.

### Allocate Memory to the Second Hard Drive

After the second hard disk is created, allocate memory to the hard disk.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open the command prompt, and type <code>diskmgmt.msc</code>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Right-click <strong>Disk 1</strong>, and click <strong>Online</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>After the disk goes online, right-click the disk, and then click <strong>Initialize Disk</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>After the disk is initialized, right-click the disk, and then click <strong>Convert to Dynamic Disk</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the <strong>Convert to Dynamic Disk</strong> window, check the <strong>Disk 1</strong> check box to select it, and then click <strong>OK</strong>. The <strong>New Simple Volume Wizard</strong> window appears.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Next</strong> and follow the on-screen instructions to create a simple volume on the disk.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Click <strong>Finish</strong> to complete the process of allocating memory to the hard drive.</td>
</tr>
</tbody>
</table>

### Set Up Third-Party Software

#### Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server 2012 R2 on all virtual machines.

Procedure

Step 1
Mount the Microsoft Windows Server ISO image to the virtual machine.
Check the Connect at power on check box when mounting the ISO.
For more information, see Mount ISO Files, on page 20.

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. The Remote Desktop Connection dialog displays a notification that the Remote Desktop Firewall exception is enabled. Click OK.

Step 11
Open the Network and Sharing Center, and in the View your active networks section, click Ethernet.

Step 12
In the Ethernet Status window, click Properties.

Step 13
In the Ethernet Properties dialog box, configure the network settings and the Domain Name System (DNS) data:
a) Uncheck Internet Protocol Version 6 (TCP/IPv6).
b) Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
c) Select Use the following IP Address.
d) Enter the IP address, subnet mask, and default gateway.
e) Select Use the following DNS Server Address.
f) Enter the preferred DNS server address, and click OK.

Step 14
Navigate to Control Panel > System and Security > System. Follow the instructions:
a) Click Change Settings.
b) In Computer name tab, click Change.
c) Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.
d) Select Domain radio button to change the member from Workgroup to Domain.
e) Enter qualified domain name and click OK.
f) In the Windows security dialog, validate the domain credentials and click OK.
g) On successful authentication, click OK.
h) Reboot the server and sign in with domain credentials.
Restart your system for the change to take effect.

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.

---

**Note**

If you want to install Unified CCE on a multilingual version of Windows Server 2012 R2, run the Multilingual User Interface (MUI) language pack. See https://software.cisco.com/download/release.html?mdfid=268439622&flowid=46046&softwareid=280840583.

If Unified CCE language pack is applied on Chinese Windows OS 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 “á” 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**

**Step 1** Open Control Panel > Clock, Region and Language.

**Step 2** In the Region section, click **Change date, time, or number formats**.

**Step 3** Click the **Administrative** tab.

**Step 4** In the Language for non-Unicode programs section, click **Change system locale**.

**Step 5** In the **Region Settings** window, select the language that matches the display language.

**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. It also aids virtual machine management.

**Procedure**

**Step 1** From the vSphere Client, right-click the virtual machine, select **Power**, and click **Power On**.

**Step 2** Click the **Summary** tab.

In the General section, the VMware Tools field indicates whether VMware Tools are:
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.


**Before you begin**


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

**Procedure**

**Step 1** Mount the Microsoft SQL Server ISO image to the virtual machine.

**Step 2** Run setup.exe.

**Step 3** Select Installation in the left pane and then click New SQL Server stand-alone installation or add features to an existing installation. Click OK.

**Step 4** On the Product Key page, enter the product key and then click Next.

**Step 5** Accept the License Terms and then click Next.
Step 6  Optional: On the Microsoft Update page, check the **Use Microsoft Update to check for updates** check box, and then click **Next**.

**Note** 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. If there are any issues, warnings or errors appear in the **Status** column. Click the links for more information about the issues.

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

If you intend to use Outbound Option High Availability two-way replication, be sure to select the Replication feature on this page. For more information about replication, refer to the Outbound Option Guide for Unified Contact Center Enterprise.

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, associate the SQL services with the virtual account.

- For the SQL Server Agent service, in the Account Name field, select NT Service\SQLSERVERAGENT. If you have enabled Outbound Option High Availability, this account must have system administrator privilege.
- For the SQL Server Database Engine, in the Account Name field, select NT Service\MSSQLSERVER.

**Note** While you can use the Network or Local Services account instead of the Virtual account, using the Virtual account provides 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 choose the SQL Server collation that supports the Windows system locale most commonly used by your organization; for example, "Latin1_General" for English.

The collation that you select affects what is written to the database. For example, suppose you set the collation for Latin1_General, but a user at the customer site selects Chinese as the language selection at sign-in. When th user enters field values in Chinese, the application returns an unsupported characters error because the database cannot 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 reinstall 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, confirm that Named Pipes is Enabled.
d)  Right-click Client Protocols and select Properties.
e)  In the Enabled Protocols section of the Client Protocols Properties window, use the arrow buttons to arrange the protocols in the following order:

1.  Shared Memory
2.  Named Pipes
3.  TCP/IP

f)  Check the Enable Shared Memory Protocol and then click OK.
g)  In the left pane, navigate to SQL Server Network Configuration > Protocols for MSSQLSERVER.
h)  In the right pane, right-click Named Pipes and select Enable.

Note  By default, Microsoft SQL Server dynamically resizes its memory. The SQL Server reserves the memory based on process demand. The SQL server releases the memory only when other processes request it, which can cause unnecessary memory monitoring tool alerts.

Cisco supports the Microsoft validation to dynamically manage the SQL Server memory. If your solution raises too many memory alerts, you can manually limit SQL Server's memory usage. Set the maximum limit of the memory with the maximum memory usage settings in the SQL Server Properties menu.

For more information on SQL Server memory settings and use, see the Microsoft SQL Server documentation.
Step 19  Set the SQL Server's default language to English as follows:
   a) Launch SQL Server Management Studio.
   b) In the left pane, right-click the server and select Properties.
   c) Click Advanced.
   d) In the Miscellaneous section, set the Default Language to English.
   e) Click OK.

   **Important**  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 follows:
   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, change the startup type to Automatic, and click Apply.
   e) To start the service, click Start, and then click OK.

---

**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.

---

**Caution**

Do not change the SQL port number. Retain the default port numbers as 1433 for TCP and 1434 for UDP connections. In case you change the port numbers, the applications like CCEAdmin will not work.

---

**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. Complete the following steps to set a user as a System Administrator:

---

**Procedure**

**Step 1**  Open the Microsoft 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.

Note  This step is mandatory.

System administrator is a predefined fixed server-level role in the Microsoft SQL Server. The system administrator performs operations on a site-level. System administrators manage jobs, role definitions, and shared schedules that are used to run reports.

You must be a system administrator to create, modify, and delete individual records in the Configuration Manager tool.

For details about the sysadmin role, see the Microsoft SQL documentation.

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 Deep Security


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.

• The firewall component of Trend Micro Deep Security blocks communication between each side of the Router/PG.

If you retain the default (enabled) and start service on side A and B you can see a new deny event logged in Trend Micro Manager > Events> Firewall Events.

To resolve the issue, disable the Trend Micro firewall policy or add a new firewall exception for that particular policy.

To resolve the issue, disable the Symantec firewall on all Unified CCE boxes and restart the services.

If you are using a managed client, perform the following steps:

1. Launch Symantec Endpoint Protection Manager.
2. Click Policies.
3. Right-click the firewall policy that you want to disable, and then select Edit.
4. Uncheck the check mark next to the policy to disable it.
5. Click OK to confirm.

If you are using an unmanaged client, perform the following steps:

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.

Install .NET Framework 4.5.2

The Unified CCE installation or upgrade runs faster if .NET Framework 4.5.2 or later version is pre-installed. If the appropriate version of the .NET Framework is not installed, the Unified CCE installer installs it.

Configure a Database Drive

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

Procedure

Step 1 Start > All Programs > Administrative Tools > Computer Management.
Step 2  In the left pane, expand Storage and click Disk Management.
Step 3  On the Disk Management window, in the left pane, right-click Disk 1, and then select Online.
Step 4  Right-click Disk 1 again, and select Initialize Desk.
Step 5  In the Initialize Desk window, for the Use the following partition style for the selected disks: option, choose the MBR (Master Boot Record) radio button.
Step 6  To create a new disk partition, right-click the right pane corresponding to Disk 1 and select New Simple Volume.
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.
Installation

• Installation Task Flow, on page 31
• Installation Tasks, on page 33

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 33</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 11.6(1) Software, on page 35</td>
</tr>
<tr>
<td>Install Outbound Option</td>
<td>Create Outbound Option Database, on page 39 and then see</td>
</tr>
<tr>
<td></td>
<td>Outbound Option Guide for Unified Contact Center Enterprise at</td>
</tr>
<tr>
<td></td>
<td>unified-contact-center-enterprise/products-user-guide-list.html</td>
</tr>
<tr>
<td>Install Finesse</td>
<td>Cisco Finesse Server Installation, on page 59</td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

or

Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 76 |
| Install Live Data Standalone (4000, 8000, 12000 Agent Deployment) or Install Coresident Deployment (2000 Agent Deployment) | Live Data Standalone Installation, on page 69

or

Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 76 |

and

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.

Set Up Virtual Machines for Installation

Validate Network Adapter Settings and Power On

Procedure

| Step 1 | Select the virtual machine (VM) in the vSphere client. Right-click the VM and choose Edit settings. |
| Step 2 | On the Hardware tab, select each network adapter. Make sure that Connect at power on in the Device Status group is checked. |
| 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.

---

### Table: Installation Tasks

<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.
2 UCCE 11.6(1) supports only Cisco MediaSense 11.5.
Configure Network Cards

**Procedure**

**Step 1** In the virtual machine, open Network and Sharing Center.

**Step 2** Click *Change adapter settings*.

**Step 3** Rename Ethernet to *visible* for the Public network card.

**Step 4** Rename Ethernet 2 to *private* for the Private network card.

**Step 5** Press *Alt* to display the menu bar, and on the Advanced menu, click *Advanced Settings*.

**Step 6** Click the Adapters and Bindings tab, and in the Connections list, sort the connections so that *visible* is on top, and then click *OK*.

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.

  **Note** 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.

  **Note** 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.

Note 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.

**Install Unified CCE 11.6(1) Software**

Before installing Unified CCE Release 11.6(1), you must install Unified CCE Release 11.0(1). While installing Unified CCE Release 11.0(1), you can perform an in-line upgrade to Unified CCE Release 11.6(1).

**Before you begin**

Download the Unified CCE Release 11.6(1) installer from the Unified CCE Download Software page on Cisco.com.

**Procedure**

**Step 1** Mount the Unified CCE Installer ISO image to the virtual machine. For more information, see Mount ISO Files, on page 20.

**Step 2** Open the ICM-CCE-CCHInstaller/AdminClientInstaller run Setup.exe. In case if you are using AdminClientInstaller skip to step 4 and click Next.

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

**Step 4** To apply the CCE Release 11.6(1) minor release, click Browse and navigate to the Unified CCE Release 11.6(1) installer. Click Next, and follow the onscreen instructions.

You can also proceed with the installation of Release ICM 11.0(1) without selecting the Release ICM 11.6(1) installer in this step. After installing Release ICM 11.0(1), double-click the Release ICM 11.6(1) installer, and proceed from step 7.

**Step 5** Reboot the server when the installation is complete.

**Step 6** Log in to your system using domain credentials with administrative privileges.

**Step 7** Wait for the Unified CCE Release 11.6(1) installation wizard to launch. Click Next to proceed.

**Step 8** Select the radio button to accept the license agreement and click Next.

**Step 9** Click Install to begin the installation.
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
Log in with administrator privilege and open the Domain Manager Tool.

Step 2
Choose the domain.

Step 3
If this OU is the first instance, then perform the following steps to 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 Create Database dialog box, click **Add** to open the Add Device dialog box.

d) Click **Data**.

e) Choose the drive on which you want to create the database, for example, the E drive.

f) 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.

g) Click **OK** to return to the Create Database dialog box.

h) Click **Add** again.

i) In the Add Device dialog box, click **Log**.

j) Choose the drive where you created the database.

k) In the **Size** field, choose the default setting or, if you have calculated an appropriate size for your deployment, enter that value.

l) 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 or the Side B Logger.

**Create Administration and Data Server Database**

**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 or LoggerB. 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.
- **Step 5**: Click Data, and choose the drive on which you want to create the database, for example, the E drive. Leave the DB size with default value and click OK to return to the Create Database dialog box.
- **Step 6**: 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 7**: 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; both logger machines must be up and operational.

**Before you begin**

If you choose to enable Outbound Option, you can also enable Outbound Option High Availability. Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Use the ICMDBA tool to create an outbound database on Side A and Side B; then set up the replication by using the Web Setup tool, as described in several of the following steps.
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 these interfaces: Router Private and Logger Private. Then, click Next.

**Step 5**  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 6**  On the Additional Options page, click Display Database Purge Configuration Steps.

**Step 7**  Click the Enable Outbound Option check box if you are installing a Unified CCE Logger and choose to deploy Outbound Option.

**Note**  If this Logger is being added for a Rigger server, where there are two IP addresses that are configured on the visible Network Interface Card (for IP-based prioritization), uncheck "Register this connection’s addresses in DNS" for the visible ethernet card. In addition, ensure that there is only one A-record entry in the DNS server corresponding to the host name of the server, which maps to the normal priority IP address. This is necessary for processes like the campaign manager and replication running as part of the Logger service, to listen on the right interface IP address for client connections.

**Step 8**  Click the Enable High Availability check box to enable Outbound Option High Availability on the Logger. (An Outbound Option database must exist on Logger Side A and Logger Side B.) Checking this check box enables Outbound Option High Availability two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Two-way replication requires that you check this check box on both the Logger Side A and Side B Additional Options page. If you disable two-way replication on one side, you must also disable it on the other side.

You must enable Outbound Option in order to enable Outbound Option High Availability. Similarly, if you want to disable Outbound Option and you have enabled Outbound Option High Availability, you must disable High Availability (uncheck the Enable High Availability check box) before you can disable Outbound Option (uncheck the Enable Outbound Option check box).

**Step 9**  If you enable High Availability, enter a valid public server hostname address for Logger Side A and Logger Side B. Entering a server IP address instead of a server name is not allowed.

**Step 10**  If you enable High Availability, enter the SQL Server Admin Credentials (Username and Password), which are required to establish two-way replication. The username and password must be the same on Logger Side A and Logger Side B, and the user must have the SQL Server System Admin privilege.

SQL replication requires that the correct SQL system admin username and password be in place when setting up Outbound Option High Availability. Changing the password for the SQL user used to set up SQL replication in Outbound Option High Availability causes replication to fail until you disable High Availability and re-enable it with the new username and password. Because of this requirement, be careful about how and when you change the password for this user.

**Step 11**  Select the Syslog box to enable the Syslog event feed process (cw2kfeed.exe).
The event feed is processed and sent to the Syslog collector only if the Syslog collector is configured. For more information about the Syslog event feed process, see the Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

**Note**

- Click **Next**.

**Step 13** On the Data Retention page, modify the Database Retention Configuration table:
  
a) For these tables, set the retention period to 40 days:
  
  - Application_Event
  - Event
  - Network_Event
  - Route_Call_Detail
  - Route_Call_Variable
  - Termination_Call_Detail
  - Termination_Call_Variable

  b) Accept the default settings for all other tables. If your contact center requires access to any of that data for a longer period, enter an appropriate value.

**Step 14** Click **Next**.

**Step 15** On the Data Purge page, configure purges for a day of the week and a time when there is low demand on the system.

**Step 16** Accept the default **Automatic Purge at Percent Full**.

**Step 17** Click **Next**.

---

### 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** On the **Deployment** page, choose the current instance.

**Step 4** In the **Deployment** dialog, select the appropriate side.

**Step 5** Click **Duplexed**, and then click **Next**.

**Step 6** In the **Router Connectivity** dialog, configure the Private Interface and Public (Visible) Interfaces. Click **Next**.
For the address input fields, use Fully Qualified Domain Names instead of IP addresses.

When there are two IP addresses configured on the visible Network Interface Card (for IP-based prioritization), manually add two A-records on the DNS server. One A-record is for the high priority IP address and the other one is for the normal priority IP address. The host part of the two DNS entries should be different from the hostname of Windows server. Use the new DNS entries to configure the visible interfaces. This note applies to the Router and to all PG machines.

**Step 7**

In the **Enable Peripheral Gateways** field, enter the number assigned to the PGs to enable it. Click **Next**.

Use a hyphen to indicate a range and commas to separate values. For example, "2-4, 6, 79-80" enables PG2, PG3, PG4, PG6, PG79, and PG80. Spaces are ignored.

**Step 8**

In the **Router Options** dialog, the **Enable Quality of Service (QoS)** is enabled by default. Click **Next**.


**Step 9**

In the **Router Quality of Service** dialog, click **Next**.

**Step 10**

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><strong>Administration &amp; Data Server type</strong></th>
<th><strong>Choose</strong></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:

- 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 the name of the site.

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 the name if the site.

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`.

---

**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 (UCC Enterprise Gateway PG)

**Configure Peripheral Gateways in PG Explorer**

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.

**Before you begin**

Ensure that the Logger, Router, and Distributor services are running.

**Procedure**

**Step 1**  
From your desktop, double-click the Unified CCE Tools icon, and then select Administration Tools.

**Step 2**  
Double-click the Configuration Manager icon.

**Step 3**  
Select `Tools > Explorer Tools > PG Explorer Tool`.

**Step 4**  
Click `Retrieve`, then click `Add PG`.

**Step 5**  
Complete the Logical Controller section as follows:
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
   - Configure Agent Desk settings before adding CUCM PG. See Assign Agent Desk Settings
   - For a VRU PG: VRU

Step 6
Do not exit the PG Explorer tool. You add a peripheral to the PG and save the configuration in the next procedure.
Configure Network VRU before adding VRU PG. See Configure Network VRUs, on page 103

- 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:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administration &amp; Data Server site name</strong></td>
<td>The name of the currently selected site in the agent distribution entries list. For MR PGs, do not specify a name for this field.</td>
</tr>
<tr>
<td><strong>Agent real time data</strong></td>
<td>Check to enable the flow of agent real-time data from the peripheral to the Administration &amp; Data Server. Uncheck to disable the flow of agent real-time data.</td>
</tr>
<tr>
<td><strong>Agent historical data</strong></td>
<td>Check to enable the flow of agent historical data from the peripheral to the Administration &amp; Data Server. Uncheck to disable the flow of agent historical data.</td>
</tr>
</tbody>
</table>

**Step 5**
On the Routing Client tab, enter the following:
a) **Name**—An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.
b) **Timeout threshold**—The maximum time, in milliseconds, the routing client can wait for a response to a routing request.
c) **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.
d) **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.
e) **Default media routing domain**—Retain the default value, which is **None**.
f) **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.

g) **Configuration parameters**—Leave blank.
h) **Dialed 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.
i) **Client Type**—Select as follows from the drop-down list:
   - For a CUCM PG: IPCC/Enterprise Agent
   - For a VRU PG: VRU
   - For an MR PG: MediaRouting
   - For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

j) **Description**—More information about the routing client.

k) **Network routing client**—A name used to associate routing clients across instances.

l) **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 Gateway Setup**

For MR PGs, 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**  
Click **Add** in the Instance Components section.

**Step 3**  
Click **Peripheral Gateway**.

**Step 4**  
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 simplex, 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 5**  
Click **Add**, and then click **Next**.

**Step 6**  
Enter the Logical Controller ID generated while configuring the PG in the **PG Explorer** tool. Click **Add** and select **PIM 1** from the list. Click **OK**.
Step 7 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. Usually, 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 in the Peripheral ID field. This is the ID that you created when you configured the PG in the PG Explorer tool.

d) For CUCM PG:

1. Enter the Agent extension length.

2. In the CUCM Parameters section, in the Service field, provide the IP address of the CUCM.

3. Enter the credentials of Application User that you created in CUCM.

4. Select the appropriate Mobile Agent Codec, and click OK.

e) For MR PG:

1. Enter the hostname or the IP address of the multichannel application server machine in the Application Hostname (1) field. If you are configuring the Outbound Option PIM, enter the IP address or hostname of the BA_IP Dialer.

2. For Outbound Option, enter the connection port for the BA_IP Dialer in the Application Connection Port (1) field. Otherwise, accept the default port number (38001) on the application server machine that the PIM uses to communicate with the application.

3. If two applications interact with the Unified CCE, in the Application Hostname (2) field, 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.

4. For two applications that interact with the Unified CCE, in the Application Connection Port (2) field, enter the port number on the second application server machine that is used by the PIM.

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

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

e) For VRU PG:

1. In the VRU host name field, enter the name by which the VRU is known to the network.

2. In the VRU connect port field, enter the number of the VRU connection port that the PG connects to.

3. In the Reconnect interval (sec) field, specify how often, in seconds, the PG tries to re-establish a lost connection to the VRU. The default value is usually appropriate.

4. In the Heartbeat interval (sec) field, specify how often, in seconds, the PG checks its connection to the VRU. The default value is usually appropriate.

5. In the DSCP field, use the drop-down box to override the default value and set it to the desired DSCP value. The list of DSCP values in the drop-down box are the same as what are used during setup for
connection between the Peripheral Gateway (PG) and the CallRouter. On an existing VRU PG system, this registry key does not exist. In that scenario, the PIM code uses CS3 as the default value when the VRU PIM process is activated.

Step 8  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)  Configure the Private Interface and Public (Visible) interfaces and click Next.
   
   **Note:**
   
   For the address input fields, use Fully Qualified Domain Names instead of IP addresses.
   
   When there are two IP addresses configured on the visible Network Interface Card (for IP-based prioritization), manually add two A-records on the DNS server. One A-record is for the high priority IP address and the other one is for the normal priority IP address. The host part of the two DNS entries should be different from the hostname of Windows server. Use the new DNS entries to configure the visible interfaces. This note applies to the Router and to all PG machines.

Step 10 In the **Check Setup Information window**, 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 Application>Plugins. 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 When prompted for the TFTP Server IP address, enter the CUCM IP address.
Step 11 Click Finish.
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, and click OK.
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.

Step 6
Click Save.

Step 7
Select Component Management > Administration Clients.
Step 8    Click Add.
Step 9    Select an instance for the Administration Client from the drop-down list.
Step 10   Click the radio button for your Administration Client type.
Step 11   Enter the hostname or IP address of the Primary and Secondary Administration & Data Servers. If you have only one Administration & Data Server, specify it for both Primary and Secondary Administration & Data Servers; both fields are required.
Step 12   Click Save.

Install Unified CCE Language Pack

The Unified CCE Language pack is used to install the localized version of the help files of the Unified CCE Web Administration tool.

The Unified CCE Language pack also contains the customized version of Configuration Manager tools for east Asian locales like Chinese, Japanese and Korean. The language pack enables localized input to be entered in those Configuration Manager tool sets.

These tool sets include some of the following tools:

- Explorer Tools
- List Tools
- System Information
- Outbound Option related tools

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\jre1.8.0_66) 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.


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 see 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.
The ICM-CCE-Installer installs the version of Java that is listed in the *Unified CCE Solution Compatibility Matrix*. If an older version of JRE is currently installed on the deployment machine, the installer does not uninstall it.

---

**Upgrade Tomcat Utility**

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 7.0 build releases. (That is, only version 7.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 7.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 7.0.62 to 7.0.65. You cannot use this tool for major or minor version upgrades.

- Revert a Tomcat upgrade.

  We do not guarantee compatibility with the latest build release of Tomcat. If upgrading Tomcat causes a problem, use the utility to revert to the previous release.

---

**Note** If you use the utility to upgrade Tomcat multiple times, you can revert to only one version back of Tomcat. For example, if you upgrade Tomcat from 7.0.62 to 7.0.63, and then to 7.0.75, the utility reverts Tomcat to 7.0.63.

---

Before using the tool:


- Download the utility (UpgradeTomcatTool-<version>.jar) and copy it onto the Unified CCE component VMs.

  Download link: https://software.cisco.com/download/release/html?mid=24360381&did=46710&softwareid=24416107&release=11.6(1)&refid=AWAREABLE&lifecycle=&reltype=latest

- Delete or back up large log files in these directories to reduce upgrade time:
  
  c:\icm\tomcat\logs
  c:\icm\debug.txt

---

**Upgrade Tomcat**

For detailed information on the results from each step, see the ../UpgradeTomcatResults/UpgradeTomcat.log file.
Procedure

Step 1 From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.

Step 2 Enter this command to run the tool: `java -jar UpgradeTomcatTool-<version>.jar -upgrade`  
For example:  
```
java -jar UpgradeTomcatTool-11.5.1.jar -upgrade
```

Step 3 When prompted, enter the full pathname of the new Tomcat installer.  
For example:  
```
c:\tomcatInstaller\apache-tomcat-7.0.75.exe
```

Step 4 When prompted, enter `yes` to continue with the upgrade.

Step 5 Repeat these steps for all unified CCE component VMs.

Silent installation

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

Silent Installation Prerequisites for Unified CCE Release 11.0(x)

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-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 for Unified CCE Release 11.0(x)

**Procedure**

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

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

Silent Installation Prerequisites for Unified CCE Release 11.6(x)

Before running a silent installation, complete the following tasks:

- Stop all applications that are running on the system.

- The machine on which you create your response file should have a configuration that closely matches the machines on which you will run silent installs. This minimizes the chances of unexpected dialogs being triggered during the installation that could terminate the installation.

For example, if the response file is created on a machine with Unified CCE services set to Manual and then run on a machine with those services set to Automatic, an additional dialog will open during the install (alerting you that the services have been set from Automatic to Manual). This unexpected dialog will cause the install to terminate, potentially leaving the system in an invalid state that requires manual recovery.

Perform a silent installation for Unified CCE Release 11.6(x)

**Procedure**

**Step 1** Run `setup` from a command prompt with two command line arguments to create the response file.

**Example:**

```
c:\ICM11.6(1).exe" -r -f1c:\myanswerfilename.iss
```

The `-r` flag is for recording the response file.

The `-f1` flag is the full path and filename for the resulting response file to be created.

**Note**

There is no space between the `-f1` and the start of the file path. If no `-f1` flag is present, the response file is written to a default location (C:\Windows)".
When you have navigated through the setup process (which completes a full installation of the product on the machine recording the response file) the resulting response file can be copied to any additional machine during a silent installation.

**Step 2**

Run setup from a command prompt using the same syntax as listed in step 1, with one exception: use `-s` instead of `-r` to indicate the install should run silently using the response file found at `-f1` filepath.

**Example:**
```
c:\ICM11.6(1).exe" -s -f1:\myanswerfilename.iss -f2:\silentinstall.log
```

The `-f2` flag creates a log file.

---

**What to do next**

Verify that the silent installation was successful by checking the installer log file to make sure no errors were reported. If your silent installation does not run, check the log file for `ResultCode=-5`. It indicates the installer could not find your response file; recheck your path and file names.

During the creation of the response file, if you chose not to reboot the machine after the installation, ensure that you manually reboot any silently installed system prior to starting the services.

---

**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**

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.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Press this key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move to the next field</td>
<td>Tab</td>
</tr>
<tr>
<td>Move to the previous field</td>
<td>Alt-Tab</td>
</tr>
<tr>
<td>Select an option</td>
<td>Spacebar</td>
</tr>
<tr>
<td>Scroll up or down a list</td>
<td>Up or Down Arrow keys</td>
</tr>
<tr>
<td>Go to the previous screen</td>
<td>Tab to Back and press the Spacebar</td>
</tr>
<tr>
<td>Get information about a screen</td>
<td>Tab to Help and press the Spacebar</td>
</tr>
</tbody>
</table>

**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>Step</th>
<th>Task Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install Finesse on the primary node.</td>
<td>See Install Finesse on Primary Node, on page 60.</td>
</tr>
<tr>
<td>2</td>
<td>Configure the CTI server settings.</td>
<td>See Configure Contact Center Enterprise CTI Server Settings, on page 63.</td>
</tr>
<tr>
<td>3</td>
<td>Configure the database settings.</td>
<td>See Configure Contact Center Enterprise Administration &amp; Data Server Settings, on page 64.</td>
</tr>
<tr>
<td>4</td>
<td>Configure the cluster settings for the secondary node.</td>
<td>See Configure Cluster Settings, on page 65.</td>
</tr>
<tr>
<td>5</td>
<td>Restart Cisco Finesse Tomcat on the primary node.</td>
<td>See Restart Cisco Finesse Tomcat, on page 65.</td>
</tr>
<tr>
<td>6</td>
<td>Install Finesse on the secondary node.</td>
<td>See Install Finesse on Secondary Node, on page 65.</td>
</tr>
<tr>
<td>7</td>
<td>Ensure replication is functioning between the two nodes.</td>
<td>See Check Replication Status, on page 69.</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. For more information, see the section on *Installation Files*.

**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 **OK** on the Disk 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
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 into the Finesse administration console on the primary Finesse server (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 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.

**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 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.
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>
</tbody>
</table>

**Note**
Because Finesse expects the primary and backup Administration & Data Server ports to be the same, the Finesse administration console exposes only one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
### 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>If you are not already signed in, sign in to the administration console with the Application User credentials.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the Cluster Settings area, in the Hostname field, enter the hostname of the secondary Finesse server.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Access the CLI and run the following command: <code>utilsservicenrestartCiscoFinesseTomcat</code></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>You can enter the command <code>utilsservicelist</code> to monitor the Cisco Finesse Tomcat Service. After Cisco Finesses Tomcat changes to STARTED, agents who have passwords can sign in to the desktop.</td>
</tr>
</tbody>
</table>

### 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.
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. See *Install Finesse on Primary Node*.
- 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 **Host Name** of the primary Finesse server.
b) Enter the **IP Address** of the primary Finesse server.
c) Enter the **Security Password** of the primary Finesse server.
d) Confirm the **Security Password**.
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.

Note  To access platform specific applications like Disaster Recovery System, Cisco Unified Serviceability, and Cisco Unified Operating System Administration, use the following URL, https://FQDN of Finesse server:8443.

Upgrade VMware Tools

To install or upgrade VMware Tools using VOS, for both nodes of Cisco Finesse, perform the following steps:

Procedure

Step 1  Power on the virtual machine.

Step 2  Right-click the VM menu. Select Guest > Install / Upgrade VMware tools.

Step 3  Select the interactive tools update and click OK.

Step 4  Open the console and log in to command prompt.

Step 5  Enter the command `utilsvmttools refresh` and confirm. The server automatically reboots twice.

Step 6  After reboot, check the Summary tab for the VM to verify whether the VMware Tools version is current. If it is not current, reboot the VM and check the version again. The process takes a few minutes. After the process is completed, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.
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:

```bash
utils dbreplication runtimestate
```

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

---

Live Data Standalone Installation

Follow this sequence of tasks to install Live Data Standalone.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set Deployment Type in Unified CCE Administration Configuration, on page 69</td>
</tr>
<tr>
<td>2</td>
<td>For all deployments except the 2000 agent reference design, verify that you created a separate virtual machine for the IDS publisher node and the IDS subscriber node. See Set Up Virtual Machines, on page 16.</td>
</tr>
<tr>
<td>3</td>
<td>Install Live Data Primary Node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 70</td>
</tr>
<tr>
<td>4</td>
<td>Set Live Data Secondary Node, on page 71</td>
</tr>
<tr>
<td>5</td>
<td>Install Live Data Secondary Node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 72</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade VMware Tools. See Install VMware Tools, on page 73</td>
</tr>
<tr>
<td>7</td>
<td>Configure Live Data with AW, on page 73</td>
</tr>
<tr>
<td>8</td>
<td>Configure Live Data Machine Services, on page 75</td>
</tr>
<tr>
<td>9</td>
<td>Configure Live Data for Unified Intelligence Center Data Sources, on page 75</td>
</tr>
<tr>
<td>10</td>
<td>Restart Live Data, on page 76</td>
</tr>
<tr>
<td>11</td>
<td>Set Up Certificates for Live Data, on page 76</td>
</tr>
</tbody>
</table>

---

Set Deployment Type in Unified CCE Administration Configuration

Before you install or upgrade Live Data you must set the deployment type.
Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

**Procedure**

**Step 1** Navigate to Unified CCE Administration > System > Deployment.

**Step 2** Select your deployment from the drop-down menu and click Next.

---

**Procedure**

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine, power it on, and open the console.

**Step 4** Follow the Install wizard, making selections as follows:

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

b) In the Success screen, select OK.

c) In the Product Deployment Selection screen:
   - For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option Cisco Unified Intelligence Center with Live Data and IdS, and then select OK. The Cisco Unified Intelligence Center with Live Data and IdS option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.
   - For all other deployments, select one of the standalone install options. For example, select Cisco Unified Intelligence Center, Live Data, or Cisco Identity Service (IdS). 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.

**Note** For Live Data servers, use the same timezone for all the nodes.
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, click Yes to enable DNS client.

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.

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

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

Step 5  Unmount the ISO image.

---

Set Live Data Secondary Node

Use the set live-data secondary command to provide the primary node the address of the secondary node.

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

Related Topics

set live-data secondary, on page 251
## Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

### Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Virtualized Voice Browser, Cisco MediaSense, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

---

**Note**

If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

### Procedure

| Step 1 | Create a virtual machine for your VOS-based contact center application using the OVA. |
| Step 2 | Mount the ISO image for the software to the virtual machine. |
| Step 3 | Select the virtual machine and power it on. |
| Step 4 | Follow the Install wizard, making selections as follows: |
|       | a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity. |
|       | b) In the **Success** screen, select **OK**. |
|       | c) In the **Product Deployment Selection** screen: |
|       | • For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server. |
|       | • For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center**, **Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**. |
| Step 5 | Follow the Install wizard, making selections as follows: |
|       | a) In the **Proceed with Install** screen, select **Yes**. |
|       | b) In the **Platform Installation Wizard** screen, select **Proceed**. |
|       | c) In the **Apply Patch** screen, select **No**. |
|       | d) In the **Basic Install** screen, select **Continue**. |
|       | e) 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**. |
|       | **Note** For Live Data servers, use the same timezone for all the nodes. |
|       | f) In the **Auto Negotiation Configuration** screen, select **Continue**. |
|       | g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units. |
|       | h) In the **DHCP Configuration** screen, select **No**. |
i) In the Static Network Configuration screen, enter static configuration values. Select OK.

j) In the DNS Client Configuration screen, enter your DNS client configuration. Select OK.

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

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

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

n) In the warning screen, select OK.

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

p) 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.

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

r) In the Platform Configuration Confirmation screen, select OK. The installation begins and runs unattended.

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

   • The installation ends at a sign-in prompt.

Step 6  Unmount the ISO image.

---

**Install VMware Tools**

To install or upgrade VMware Tools using VOS, for both nodes of Live Data, perform the following steps:

**Procedure**

---

**Step 1**  Ensure that your virtual machine is powered on.

**Step 2**  Right-click the VM menu. Select Guest > Install / Upgrade VMware tools.

**Step 3**  Choose the interactive tools update and press OK.

**Step 4**  Open the console and log in at the command prompt.

**Step 5**  Enter the command `utilsvmttools refresh` and confirm. The server automatically reboots twice.

**Step 6**  After reboot, check the Summary tab for the VM to verify that the VMware Tools version is current. If it is not current, reboot the VM and check the version again.

The process takes a few minutes. After the process completes, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

---

**Configure Live Data with AW**

Configure Live Data with AW 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 to perform the test. When you include the skip-test parameter, the command does not check if the configured user has appropriate AW DB access and does not report results.

**Note**
You do not need to configure the AW DB on both the Publisher and the Subscriber. The configuration is replicated between the Publisher and Subscriber.

**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 126.

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:

```
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 to perform the test.)

```
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 to perform the test.)

```
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 to perform the test.)

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

For more information, see set live-data aw-access, on page 250.

**Related Topics**

- Configure SQL User Account, on page 126
- set live-data aw-access, on page 250
- show live-data aw-access, on page 251
Configure Live Data Machine Services

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

Whenever you run set live-data machine-services, be sure to also run set live-data cuic-datasource to reconfigure the Live Data data sources for the Unified Intelligence Center. See Configure Live Data for Unified Intelligence Center Data Sources, on page 75

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
```

For more information, see set live-data machine-services, on page 255.

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

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

  To populate the connection information automatically, your deployment must support Live Data. To set the deployment type, see Set Deployment Type in Unified CCE Administration Configuration, on page 69.

- Cisco Unified Communications Manager (CUCM) PG, generic PGs with CUCM peripherals, Unified CCE Gateway PGs, and Avaya PGs are supported for Live Data.

Configure Live Data for 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
```
For more information, see set live-data cuic-datasource, on page 253.

## Restart Live Data

After you complete the configuration procedures for the AW, the Live Data Machine Services, and the Unified Intelligence Center data source, restart the Live Data system to enable the changes.

### Procedure

Access the Live Data CLI and run the following command:

```
utils system restart
```

## 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 Standalone, on page 257.

## Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

Follow this sequence of tasks to install the coresident deployment (Cisco Unified Intelligence Center with Live Data and IdS).

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set Deployment Type, on page 77</td>
</tr>
<tr>
<td>2</td>
<td>Install Coresident Deployment Primary Node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 70</td>
</tr>
<tr>
<td>3</td>
<td>Install Coresident Deployment Secondary Node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 72</td>
</tr>
<tr>
<td>4</td>
<td>Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory, on page 80</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade VMware Tools. See Install VMware Tools, on page 81</td>
</tr>
<tr>
<td>6</td>
<td>Configure Live Data with AW, on page 81</td>
</tr>
</tbody>
</table>
Set Deployment Type

Before you install or upgrade, you must set the deployment type.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Navigate to Unified CCE Administration &gt; System &gt; Deployment.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select your deployment from the drop-down menu and click Next.</td>
</tr>
</tbody>
</table>

Install Publisher/Primary Nodes of Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

Heve

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Virtualized Voice Browser, Cisco MediaSense, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Note

If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a virtual machine for your VOS-based contact center application using the OVA.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Mount the ISO image for the software to the virtual machine.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the virtual machine, power it on, and open the console.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Follow the Install wizard, making selections as follows:</td>
</tr>
<tr>
<td>a)</td>
<td>In the Disk Found screen, click OK to begin the verification of the media integrity.</td>
</tr>
<tr>
<td>b)</td>
<td>In the Success screen, select OK.</td>
</tr>
<tr>
<td>c)</td>
<td>In the Product Deployment Selection screen:</td>
</tr>
<tr>
<td>•</td>
<td>For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option Cisco Unified Intelligence Center with Live Data and IdS, and then select OK. The</td>
</tr>
</tbody>
</table>
Cisco Unified Intelligence Center with Live Data and IdS option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.

- For all other deployments, select one of the standalone install options. For example, select Cisco Unified Intelligence Center, Live Data, or Cisco Identity Service (IdS). 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.

Note: For Live Data servers, use the same timezone for all the nodes.

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, click Yes to enable DNS client.
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.

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

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

Step 5: Unmount the ISO image.
Install Subscribers/Secondary Nodes of Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Virtualized Voice Browser, Cisco MediaSense, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

**Note**

If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

Procedure

**Step 1** Create a virtual machine for your VOS-based contact center application using the OVA.

**Step 2** Mount the ISO image for the software to the virtual machine.

**Step 3** Select the virtual machine and power it on.

**Step 4** Follow the Install wizard, making selections as follows:

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

b) In the **Success** screen, select **OK**.

c) In the **Product Deployment Selection** screen:

   • For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server.

   • For all other deployments, select one of the standalone install options. For example, select **Cisco Unified Intelligence Center, Live Data**, or **Cisco Identity Service (IdS)**. Then select **OK**.

**Step 5** Follow the Install wizard, making selections as follows:

a) In the **Proceed with Install** screen, select **Yes**.

b) In the **Platform Installation Wizard** screen, select **Proceed**.

c) In the **Apply Patch** screen, select **No**.

d) In the **Basic Install** screen, select **Continue**.

e) 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**.

   **Note** For Live Data servers, use the same timezone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.

g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.

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

j) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.

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

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

m) In the **First Node Configuration** screen, select **No**.

n) In the warning screen, select **OK**.

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

p) 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**.

q) In the **SMTP Host Configuration** screen, select **No**.

r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.
   - There is a reboot in the middle of the installation.
   - The installation ends at a sign-in prompt.

### Step 6

Unmount the ISO image.

---

**Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory**

**Procedure**

**Step 1**  
In Unified CCE Administration, navigate to **System > Deployment**.

**Step 2**  
Add the new machine to the System Inventory:

a) Click **Add**.
   
The **Add Machine** popup window opens.

b) From the Type drop-down menu, select the following machine type:

   CUIC LD IdS Publisher, for the coresident Unified Intelligence Center, Live Data, and Identity Service machine available in the 2000 agent reference design.

   c) In the **Hostname** field, enter the FQDN, hostname, or IP address of the machine.

   The system attempts to convert the value you enter to FQDN.

   d) Enter the machine's Administration credentials.

   e) Click **Save**.

   The machine and its related Subscriber or Secondary machine are added to the System Inventory.
What to do next

If you remove a component from your deployment, delete it from your System Inventory. If you add the component again, or add more components, add those components to the System Inventory.

Install VMware Tools

To install or upgrade VMware Tools using VOS, for both nodes of Cisco Unified Intelligence Center with Live Data and IdS, perform the following steps:

1. Ensure that your virtual machine is powered on.
2. Right-click the VM menu. Select Guest > Install / Upgrade VMware tools
3. Choose the interactive tools update and press OK.
4. Open the console and log in at the command prompt.
5. Enter the command `vtls vmttools refresh` and confirm.
   The server automatically reboots twice.
6. After reboot, check the Summary tab for the VM to verify that the VMware Tools version is current. If it is not current, reboot the VM and check the version again.

The process takes a few minutes. After the process is complete, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

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.

Note

You do not need to configure the AW DB on both the Publisher and the Subscriber. The configuration is replicated between the Publisher and the Subscriber.

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 126.

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.

```
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "<user>"
GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "<user>"
```
Configure Live Data Unified Intelligence Center Data Sources

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

Before you begin

- Ensure that AW distributor and Cisco Unified Intelligence Center Publisher are in service
- Ensure that AW DB connection information is updated on the same node, where you want to configure Live Data CUIC data source
- Configure Live Data endpoints in the Machine Service table

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
```

For more information, see set live-data cuic-datasource, on page 253.
Restart Live Data

After you complete the configuration procedures for the AW and the Unified Intelligence Center data source, restart the Live Data system to enable the changes.

Procedure

Access the Live Data CLI and run the following command:

`utils system restart`
Restart Live Data
Initial Configuration

• Initial Configuration Overview, on page 85
• Initial Configuration Task Flow, on page 85
• Initial Configuration Tasks, on page 86
• Configure SQL User Account for Outbound Options High Availability, on page 172

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 85

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 86</td>
</tr>
<tr>
<td>Configure Cisco Unified Intelligence Center</td>
<td>Configure Cisco Unified Intelligence Center, on page 124</td>
</tr>
<tr>
<td>Configure Cisco Unified Customer Voice Portal</td>
<td>Configure Cisco Unified Customer Voice Portal, on page 131</td>
</tr>
<tr>
<td>Configure Cisco Unified Communications Manager</td>
<td>Configure Cisco Unified Communications Manager, on page 143</td>
</tr>
<tr>
<td>Configure Cisco Finesse</td>
<td>Configure Cisco Finesse, on page 153</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 119

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. Double-click the Configuration Manager icon.
Configure Media Routing Domain

You must establish Media Routing Domains (MRD) for each media type that your Unified CCE System supports. A Voice MRD is installed by default with Unified CCE. You need to create MRDs for other media such as chat, email, and tasks. Additionally, if you are using Cisco Enterprise Chat and Email (ECE), you need to create media classes for ECE chat and email.


Important

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 place holder 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.
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.

---

**Note**

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 autogenerated.

**Customer.** Use the drop-down list to select the customer (Unified CCE instance) associated with the dialed number.
**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 for a call. You can specify the variable name and data type. The name must begin with the string “user.” ECC variables 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:

`user.Cisco.AcctNum`

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

**Note**

For a large corporation, you can break `<VariableDescription>` down to include the Business Unit, Division, or other organizational entities.
ECC variables follow these size rules:

- An ECC variable can be either a scalar variable or an array element, each with a maximum length of 210 bytes.

  **Note**
  
  Array types are not supported for an agent request.

- The maximum number of elements in an array is 255.
- The maximum buffer size for each scalar variable = 5 + the maximum variable length. 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 an array element) * (the maximum elements in the array). There is a null terminator for each element, and a null terminator for the array as a whole.
- Since the internal buffer which stores the variables is 2000 bytes, the total sum of all the maximum buffer sizes for each variable and each array cannot exceed 2000.

For example, if you intended to use the following:

- A scalar ECC variable with a maximum length of 100 bytes
- A scalar ECC variable with a maximum length of 80 bytes
- An ECC array with a maximum of 9 elements with each element having a maximum length of 200 bytes

Total the buffer size is: (5+100) + (5+80) + (5 + (1+200)*9) = 2004. Because this size is too large, you must change the length of one of the scalar ECC variables or the length of the array ECC variables.

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 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 Voice MRDs with Collaboration, the ECC variables are:

- user.ewm.activity.id
- user.ewm.customer.name

### 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**

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

**Step 2** Select the **Expanded call context enabled** check box.

For additional information, refer to the online Help.

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

---

**Define ECC Variables**

**Procedure**

**Step 1** Within the Configuration Manager, double-click **Tools > List Tools > Expanded Call Variable List**. The Expanded Call Variable List window appears.

**Step 2** Click **Retrieve** to enable adding ECC variables.

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

The Attributes property tab appears.

**Step 4** Complete the Attributes property tab. See the **List Tools Online Help** for details on the Attributes property tab.

**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.

  **Note**
  
  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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Within the Configuration Manager, select <strong>Tools &gt; List Tools &gt; User Variable List</strong>. The User Variable List window appears.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>In the User Variable List window, click <strong>Retrieve</strong> to enable Add.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Click <strong>Add</strong>. The Attributes property tab appears.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Complete the Attributes property tab. <strong>Note</strong> The <strong>Variable name</strong>, <strong>Object type</strong>, and <strong>Data type</strong> fields are required. All other fields are optional. For additional information refer to the online Help.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Click <strong>Save</strong> to apply your changes.</td>
</tr>
</tbody>
</table>
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.
**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.

Note

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.

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

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

---

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

**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.

---

**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 https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.html.
Step 5  Click **Save** and then click **Close**.

---

### Designate Agent Supervisor

You can identify an agent as a supervisor.

If you define an agent as a supervisor:

- If single sign-on is *disabled* either globally or for the agent you want to designate as a supervisor, the supervisor must have an Active Directory account. If the supervisor does not have an Active Directory account, the designation fails.

- If single sign-on is *enabled* either globally or for the agent you want to designate as a supervisor, you must enter the individual's name in the format that your identity provider requires.

To create an agent who is a supervisor:

**Procedure**

**Step 1**  In the Configuration Manager menu, select **Tools > Explorer Tools > Agent Explorer**. The Agent Explorer window appears.

**Step 2**  In the **Select filter data** box, select the peripheral with which the agent is to associated and click **Retrieve**. This enables the **Add Agent** button.

**Step 3**  Click **Add Agent**.

**Step 4**  In the property tabs on the right side of the window, enter the appropriate property values. Use the Agent Tab to define the agent and designate the agent as a supervisor. Use the Skill Group Membership Tab to map the agent to any skill groups. (See the Configuration Manager online help for more information.)

**Note**  An agent team can have only one primary supervisor. There is no upper limit to the number of secondary supervisors for a team. Refer to the online help for instructions on how to assign a primary supervisor.

**Step 5**  When finished, click **Save**.

---

### 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.

**Procedures**

**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 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.
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 filename; 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 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.
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 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.
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.

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:
**Media Routing Domain.** Use Cisco_Voice for agents that do not use other media. For more information, see the *Enterprise Chat and Email Installation Guide (for Unified Contact Center Enterprise)* at https://www.cisco.com/en/US/products/ps7236/prod_maintenance_guides_list.html.

**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://distributorip/cceadmin.

For more information on precision routing, see the Cisco Unified Contact Center Enterprise Features Guide at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.html

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 mortgage.</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>

Step 4 Click Save.
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 available 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.

a) Click the attributes you want to add for this agent.

b) 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>
<tr>
<td>Media Routing Domain</td>
<td>no</td>
<td>MRDs organize how requests for media are routed. The system routes calls to skill groups or precision queues that are associated with a particular communication medium; for example, voice or email. This field defaults to <em>Cisco_Voice</em>. To select a different Media Routing Domain:</td>
</tr>
<tr>
<td>Service Level Type</td>
<td>yes</td>
<td>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.</td>
</tr>
</tbody>
</table>

- **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.

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.
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
</table>
| Bucket Intervals| no       | 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: |
• **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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Click the numbered step link in the Steps panel (Step 1, Step 2, and so on). The step number popup window opens.</td>
</tr>
</tbody>
</table>
| **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 116 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 123.

**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 becomes 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:

**Procedure**

• 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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>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.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Type the new entry that you want to appear in all the fields.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Enter or Tab. This applies the change to all the records in the range and moves the focus to the next data field.</td>
</tr>
</tbody>
</table>

**Apply a Single Value to a Range of Selection-Box Fields**

To apply a single value to a range of selection-box fields:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Select the first field where you want the range to start.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Press the Shift key and hold it down for steps 3, 4, and 5.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the selection-box down arrow but keep the left mouse button held down and select the fields you want in the range.</td>
</tr>
<tr>
<td>Step 4</td>
<td>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.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click your selection.</td>
</tr>
<tr>
<td>Step 6</td>
<td>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.</td>
</tr>
</tbody>
</table>
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**

![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.
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

Step 1 In the Administration application, choose Cluster Configuration > License Management.

Step 2 Click Browse.

Step 3 Navigate to the location where the *.lic file was saved.

Step 4 Click Apply License to load the license.
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**

**Step 1** Launch Microsoft SQL Server Management Studio on the Unified CCE Administration Client workstation.

**Step 2** Navigate to **Security > Logins**, right-click **Logins** and select **New Logins**.

You use this login when you configure the data sources for Cisco Unified Intelligence Center reporting.

**Step 3** On the General Screen:

a) Enter the Login Name.

b) Select **SQL Server authentication**.

c) Enter and confirm the password.

d) Uncheck **Enforce password policy**.

**Step 4** In the Server Roles page, check the following check boxes:

- public
- securityadmin
- serveradmin
- setupadmin
- sysadmin

**Step 5** On the User Mapping page, do the following:

1. Check the **Real-time database** and **Historical database** check boxes.

2. In Database role memberships pane, check the following check boxes:

   - db_datareader
   - db_datawriter
   - db_dldadmin
   - db_owner
   - db_securityadmin
   - public

**Note** For an SQL user configured to work with Live Data, check the master database check box and the db_datareader and db_datawriter check boxes (in Database role memberships pane).
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 UserID 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 UserID 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 https://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/IP address of CUIC Publisher>:8444/ cuicui.
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. Report Designers and Report Definition Designers do not have access to the Data Sources page but can see the list of Data Sources when they create custom reports. To benefit those users, give a new Data Source a meaningful name.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for this data source.</td>
</tr>
<tr>
<td>Type</td>
<td>Choose Informix. <strong>Note</strong> Type is disabled in Edit mode.</td>
</tr>
<tr>
<td>Database Host</td>
<td>Enter the IP address or hostname 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>
<tr>
<td>Instance</td>
<td>Specify the instance name of the desired database. By default, this is cvp.</td>
</tr>
</tbody>
</table>
### Initial Configuration

#### Download Report Bundles

The following Cisco Unified Intelligence Center report bundles are available as downloads from Cisco.com [https://software.cisco.com/download/type.html?mdfid=282163829&catid=null](https://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.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timezone</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Set CVP datasource timezone configuration to UTC on CUIC.</td>
</tr>
<tr>
<td><strong>Database User ID</strong></td>
<td>Enter the user ID of the Reporting User who is configured in the Operations Console to access the Unified CVP reporting database.</td>
</tr>
<tr>
<td></td>
<td>(The cvp_dbuser account is created automatically during Unified CVP Reporting server installation.)</td>
</tr>
<tr>
<td><strong>Password and Confirm Password</strong></td>
<td>Enter and confirm the password for the database user.</td>
</tr>
<tr>
<td><strong>Charset</strong></td>
<td>Choose UTF-8.</td>
</tr>
<tr>
<td><strong>Default Permissions</strong></td>
<td>View or edit the permissions for this datasource for My Group and for the All Users group.</td>
</tr>
<tr>
<td><strong>Max Pool Size</strong></td>
<td>Select the maximum pool size.</td>
</tr>
<tr>
<td></td>
<td>Value ranges from 5-200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs.</td>
</tr>
</tbody>
</table>

**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.

---

---
• 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 ([https://developer.cisco.com/web/ccr/documentation](https://developer.cisco.com/web/ccr/documentation)).

**Import Report Bundles**

**Procedure**

**Step 1** In Unified Intelligence Center, click Reports in the left pane.

**Step 2** Click Import Report.

**Step 3** In the File Name (XML or ZIP file) field, click Browse.

**Step 4** Browse to and select the report bundle zip file, and click Open.

Select a report bundle for the version of software deployed in the contact center.

**Step 5** Select the location where you want to save the file.

**Step 6** Click Import.

**Step 7** Choose one:

- If the report or reports do not yet exist, you must provide the data source. From the **Data Source for ValueList** drop-down list, select the data source used. Then click Import.

  **Note** You must select a data source for the value list only if it does not use the same data source as the report definition. For LiveData, the Data Source for ReportDefinition should be LiveData JMS DataSource. The Data Source for ValueList should be UCCE Realtime.

- 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 Yes, Yes to All, No, or No to All.

**Configure Unified Intelligence Center Administration**

Complete the following procedure to configure Unified Intelligence Center Administration.

**Procedure**

**Step 1** Sign in to the Cisco Unified Intelligence Center Administration Console ([https://<hostname>:8443/oamp](https://<hostname>:8443/oamp)).

**Step 2** Configure the Active Directory tab under **Cluster Configuration > Reporting Configuration**.
a) For Host Address for the Primary Active Directory Server, enter the IP address of the domain controller.
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 User ID, select the required option.
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.

**Note** For more details, see the online help.

**Step 3** Configure syslog for all devices.
a) Choose Device Management > Log and Trace Settings.
b) For each host address:
   • Select the associated servers and click the arrow to expand.
   • Select the server name.
   • 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</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Start &gt; Programs &gt; Administrative Tools &gt; Server Manager</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Expand <strong>Roles</strong> in the left panel of the Server Manager window.</td>
</tr>
<tr>
<td>3</td>
<td>Expand <strong>Web Server (IIS)</strong> and select <strong>Internet Information Services (IIS) Manager</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Click the <strong>Hostname</strong> in the Internet Information Services Manager window.</td>
</tr>
<tr>
<td>5</td>
<td>Under IIS, right-click <strong>Directory Browsing</strong> and select <strong>Open feature</strong>.</td>
</tr>
<tr>
<td>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</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1     | Install the FTP Service on the server.  
  a) Choose **Start > Administrative Tools > Server Manager**.  
  b) Expand **Roles** in the left panel of the Server Manager window.  
  c) Right-click **Web Server (IIS)** and click **Add Role Services**.  
  d) Check the **FTP Server** check box and then click **Install**, installation takes a few moments.  
  e) When the installation is complete, click **Close**. |
| 2     | Enable the FTP Service on the server.  
  a) Choose **Start > Administrative Tools > Server Manager**.  
  b) Expand **Roles** in the left panel of the Server Manager window.  
  c) Expand **Web Server (IIS)** and then click **Internet Information Services (IIS) Manager**.  
  d) Expand hostname.  
  e) Right-click **Sites** and click **Add FTP Site**.  
  f) Enter a **FTP site name**.  
  g) Enter `c:\inetpub\wwwroot` in the **Physical path** of the FTP site name, and click **Next**.  
  h) Enter the IP address of the CVP Server.  
  i) Select **No SSL** in SSL Options and then click **Next**.  
  j) Check the **Anonymous** and **Basic** check boxes.  
  k) Select **All Users** from the Allow Access To drop-down list.  
  l) Check the **Read** and **Write** check boxes, and then click **Finish**. |
| 3     | Set the Basic Setting for the FTP Server.  
  a) Click **Sites** and then click the FTP server that you have created.  
  b) Click **Basic Settings** in the Actions tab and click **Connect as**. |
c) Select **Application user (pass-through authentication)** option and click **OK** twice.

## Configure Unified CVP Reporting Server

### Create Reporting Users

Who can create a user:

- Initially, the System Application User who is the default Superuser.
- Eventually, any Superuser.

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.

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](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 [https://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html](https://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.
Sign In to Cisco Unified Intelligence Center Reporting Interface

Who can sign in to 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 in to 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.

Cisco Unified Customer Voice Protocol Reporting User Role Additions

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.

Perform the following procedure to obtain import Unified CVP report templates.

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

Procedure

Step 1
Launch the Unified Intelligence Center web application using the URL https://<CUCI ADDRESS:8444/cuicui/.

Step 2
Enter CUIC Username and Password.

Step 3
Create a folder to import the reports.
   a) Click Reports.
   b) From the toolbar, click New > Folder.
   c) Enter the folder name and click Save.

Step 4
Import the report templates.
   a) Click Reports > New > Import. You will be redirected to the CUIC legacy interface.
   b) Click Reports > Import Report.
   c) In the File Name (XML or ZIP File) field, click Browse and select the template file to import.
   d) In the Save To field, expand the Reports tree and select the folder created to import the report template.
   e) Click Import. CUIC validates the Report Definition ID in the template and successfully imports the template.

Note

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 OPSConsole page. If you are using Microsoft Internet Explorer, you will need to accept the self-signed certificate.

---

### Configure Unified CVP Call Server Component

**Note**

- There is one Unified CVP server on Side A and one Unified CVP server on side B for the 500 agent deployment.

- There are two Unified CVP servers on Side A and two Unified CVP server on side B for the 1000 agent deployment.

---

### 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 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.
   d) For CVP-2B, the primary call server is CVP-2B and the backup call server is CVP-2A.

**Step 5**  
Click the Configuration tab. In the Enable reporting for this CVP VXML Server field, click Yes to optionally enable reporting. If you do not want to enable reporting, click No.

**Step 6**  
Click the Device Pool tab. Make sure the default device pool is selected. If prompted to restart the primary and secondary call servers, click No. Do not restart at this time.

**Step 7**  
Click Save & Deploy.

**Step 8**  
Repeat this procedure for all CVP Servers.

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 SignIn 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 into 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

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 Password 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.
Add Unified Communications Manager Devices

Procedure

Step 1 Log in to the CVPOperationsConsole.
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 CVPOperationsConsole.
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.
Transfer Scripts and Media Files

Create the notification destination and deploy to all of the Unified CVP devices.

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **Bulk Administration > File Transfer > Scripts & Media**.

Step 2 In the Select device type field, select the **Gateway**.

Step 3 Move all Gateways to **Selected**.

Step 4 Click **Default Gateway files**.

Step 5 Click **Transfer** and select **OK** at the popup window.

Step 6 Click **File Transfer Status** to monitor transfer progress.

Configure SNMP


Procedure

Step 1 In the Unified CVP Operations Console, navigate to **SNMP > V1/V2c > Community String**.

Step 2 Click **Add New**.

a) On the **General** tab, name the community string.

b) On the **Devices** tab, select the required device from the list of available devices.

c) Click **Save and Deploy**.

Step 3 Create the notification destination and deploy to all of the Unified CVP devices.

a) Navigate to **SNMP > V1/V2c > Notification Destination**.

b) Click **Add New**.

c) Complete the fields.

d) Select the **Devices** tab and assign the SNMP notification destination to a device.

e) Click **Save and Deploy**.

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.

---

**Validate Clusterwide Domain Configuration**

This validation is required for running calls.

**Procedure**

**Step 1**  
In the Cisco Unified CM Administration, navigate to System > Enterprise Parameters.

**Step 2**  
Scroll down to Clusterwide Domain Configuration.

Cluster Fully Qualified Domain Name should match the Server Group name in the Unified CVP SIP Server Groups Configure SIP Server Group, on page 140.

**Configure Dialed Number Patterns**

Dialed number patterns are required for:
Configure Dialed Number Patterns

• 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 following table:
  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>
</table>
| 91*                   | Ringtone    | Check Enable Local Static Route.  
Route to SIP Server Group and IP 
Address/Hostname/Server Group Name are both VXML 
Gateway (for example, vxmlgw.cisco.com).  
Check Enable Send Calls to Originator. |
| 92*                   | Error       | Check Enable Local Static Route.  
Route to SIP Server Group and IP 
Address/Hostname/Server Group Name are both VXML 
Gateway (for example, vxmlgw.cisco.com).  
Check Enable Send Calls to Originator. |
| The agent extension    | Agent Device. | Check Enable Local Static Route.  
Route to SIP Server Group and IP 
Address/Hostname/Server Group Name are both the 
Unified Communications Manager gateway.  
Check Enable RNA Timeout for Outbound Calls. The 
default timeout value is 60 seconds. |
| 777*                  | Network VRU Label | Check Enable Local Static Route.  
Route to SIP Server Group and IP 
Address/Hostname/Server Group Name are both VXML 
Gateway (for example vxmlgw.cisco.com).  
Check Enable Send Calls to Originator. |
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.
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 User ID that you entered in Set Up Enterprise Parameters, on page 148. 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 Unified CVP routing clients as follows:
   a) Click **Add New**.
   b) In the **Route Pattern** field, enter `7777777777`!
   c) In the **Gateway/Route List** field, choose **SIPTRK_to_CVP_1**.
   d) Click **Save**.

**Step 3**  Add a route pattern for the Cisco Unified Communications Manager routing client.
   a) Click **Add New**.
   b) In the **Route Pattern** field, enter `8881111`!
   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.
Set Up Conference Bridge

Procedure

Step 1 Choose Media Resources > Conference bridge.
Step 2 Add a conference bridge for each ingress/VXML combination gateway in the deployment.
Step 3 In the Conference Bridge name field, enter a unique identifier for the conference bridge name that coincides with the configuration on the gateway.
Step 4 Click Save.
Step 5 Click Apply Config.

Set Up Media Termination Point

Procedure

Step 1 Choose Media Resources > Media Termination Point.
Step 2 Add a media termination point for each ingress/VXML combo gateway in the deployment.
Step 3 In the Media Termination Point Name field, enter a media termination point name for each ingress/VXML combo gateway in the deployment.
Step 4 Click Save.
Step 5 Click Apply Config.

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.
### 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 143.

**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. For more information, see Set Up Trunk, on page 144.

**Step 16** From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.
Set Up Enterprise Parameters

Procedure

Step 1
Choose System > Enterprise Parameter.

Step 2
Configure the Cluster Fully Qualified Domain Name.

Example:
ccm.hescc.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

Step 1
In Unified Communications Manager Administration, choose Device > Phone.

Step 2
Click Add a New Phone.

Step 3
Select CTI Port from the Phone Type drop-down list.

Step 4
Click Next.

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.

Step 6
In Description, enter text identifying the local CTI Port pool.

Step 7
Use the Device Pool drop-down list to choose the device pool to which you want network CTIPort pool assigned. (The device pool defines sets of common characteristics for devices.)

Step 8
Click Save.

Step 9
Highlight a record and select Add a New DN.

Step 10
Add a unique directory number for the CTI port you just created.

Step 11
When finished, click Save and Close.
Initial Configuration

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 info > 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:

Step 12 Repeat the preceding steps to configure the network CTI Port pool.
Step 13 In Device Name, enter a unique name for the local CTI Port pool name; click OK when finished.
   Use 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.
Step 14 In Description, enter text identifying the network CTI Port pool.
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.)
Step 16 Click Save.
Step 17 Highlight a record and select Add a New DN.
Step 18 Add a unique directory number for the CTI port you just created.
Step 19 When finished, click Save and Close.
**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, follow these configuration steps on Unified Communications Manager. This is required for deployments that have agents using phones that require Join Across Line (JAL) to be enabled.

Note

Use of JAL and DTAL phone features is deprecated. Do not use these features in new deployments.

Multiline Agent Control supports a maximum of four lines per phone, one ACD line and up to three non-ACD lines.

Note

Unified CCE does not support shared lines for ACD or Non ACD lines. Several agents cannot share a common extension on their phones. However, one agent can have two phones that share a common second line. The agent cannot sign in on both phones at the same time.

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.

Step 2  Configure all agent phones with the following parameters:

- Busy Trigger: 1
- Maximum Number of Calls: 2

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.
Configure audio source

Procedure

**Step 1** Log in to the Cisco Unified Communications Manager Administration page.
**Step 2** Click the **Media resources** tab, and then click **MOH Audio File Management**.
**Step 3** In the MOH Audio File Management page, click **Upload File**.
**Step 4** In the Upload File window, click **Browse**, select the audio file that you want to set for Music on Hold, and then click **Open**.
**Step 5** Click **Upload File**.

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 Unified CCE routing script

Procedure

**Step 1** Log in to the Unified CCE Administrator workstation.
**Step 2** Open the Script Editor.
**Step 3** Open the script in which you want to set the caller specific Music on Hold.
**Step 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.

Step 5 Click Save.

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.

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 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.
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>
</tbody>
</table>

**Note**
Because Finesse expects the primary and backup Administration & Data Server ports to be the same, the Finesse administration console exposes only one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
Configure Cluster Settings

Configure the cluster settings for the secondary Finess node. The secondary Finess 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 Finess server.
Step 3 Click Save.

Restart Cisco Finesses Tomcat

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

Procedure

Step 1 Access the CLI and run the following command:

```
utilsservicerestartCiscoFinessesTomcat
```

Step 2 You can enter the command `utilsservicelist` to monitor the Cisco Finesses Tomcat Service. After Cisco Finesses 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 Finesses server.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 in to the AWDB.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password required to sign in to the AWDB.</td>
</tr>
</tbody>
</table>
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.

---

### 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.

For agents who use the Task Routing interface on Finesse for non-voice tasks, set the Logout non-activity time to blank.

Perform the following steps to configure Logout non-activity time for an agent:

**Procedure**

- **Step 1**  Launch the Unified CCE Configuration Manager.
- **Step 2**  Launch Agent Desk Settings List (Tools > List Tools).
- **Step 3**  Select Agent Desk Settings List.
- **Step 4**  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.
- **Step 5**  Click Save.

The modified settings are applied to all of the agents who use these agent desktop settings.
Browser Settings for Internet Explorer

If Internet Explorer is used to access the Finesse desktop, certain settings must be configured in the browser to ensure all features of Finesse work properly.

1. Disable pop-up blockers.
   Finesse does not support Compatibility View. When the desktop is running in Compatibility View, Internet Explorer renders in the standard mode for that version.

2. Configure the following privacy and advanced settings:
   1. From the browser menu, select Tools > Internet Options.
   2. Click the Privacy tab.
   3. Click Sites.
   4. In the Address of website box, enter the domain name for the Side A Finesse server.
   5. Click Allow.
   6. In the Address of website box, enter the domain name for the Side B Finesse server.
   7. Click Allow.
   8. Click OK.

3. You must enable the following security settings to allow users to sign in:
   • Run ActiveX controls and plug-ins
   • Script ActiveX controls marked as safe for scripting
   • Active scripting

To enable these settings:

1. From the Internet Explorer browser menu, select Tools > Internet Options.
2. Click the Security tab.
3. Click Custom level.
4. Under ActiveX controls and plug-ins, select Enable for Run ActiveX controls and plug-ins and Script ActiveX controls marked safe for scripting.
5. Under Scripting, select Enable for Active Scripting.

Note
If the customer is using self-signed CA (Certificate Authority) and their agents use the server's FQDN, there should not be any certificate errors or warnings when connecting to Finesse over HTTPS.

Browser Settings for Firefox

Complete the following steps to ensure Finesse behaves as expected when it is not the active window.
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.

Finesse agents can enter either their Agent ID or Login name (in the Username field of the desktop login screen) to sign in. Ensure that each agent’s Agent ID and Login name are unique across both sets of data. If one agent’s Agent ID matches another agent’s Login name, neither agent can sign in.

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.

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 Username, Password, and Extension, and then click Sign In.
If your agent is signed into the Agent Desktop in Single Sign-On Mode or Hybrid Mode, refer to the sections "Sign In to Finesse Desktop Single Sign-On Mode" or "Sign In to Finesse Desktop Hybrid Mode" in the Cisco Finesse Desktop User Guide for Unified Contact Center Enterprise.

---

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you use Internet Explorer:</td>
<td>A page appears that states there is a problem with the website's security certificate. Click <strong>Continue to this website (not recommended)</strong>. 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.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Certificate Error</strong>, and then click <strong>View Certificates</strong> to open the Certificate dialog box.</td>
</tr>
<tr>
<td></td>
<td>3. On the Certificate dialog box, click <strong>Install Certificate</strong>. This action opens the Certificate Import Wizard.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>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 &gt; Security &gt; Trusted Sites &gt; Sites).</td>
</tr>
<tr>
<td></td>
<td>After you click <strong>Install Certificate</strong>, under <strong>Store Location</strong>, select <strong>Current User</strong> to install the certificate for the current user only, or select <strong>Local Machine</strong> to install the certificate for all Windows users who use this computer.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>5. Select <strong>Place all certificates in the following store</strong>, and then click <strong>Browse</strong>.</td>
</tr>
<tr>
<td></td>
<td>6. Select <strong>Trusted Root Certification Authorities</strong>, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>7. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td></td>
<td>8. Click <strong>Finish</strong>.</td>
</tr>
<tr>
<td></td>
<td>9. If a Security Warning dialog box appears that asks if you want to install the certificate, click <strong>Yes</strong>. A Certificate Import dialog box that states the import was successful appears.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>10.</td>
<td>Click OK.</td>
</tr>
<tr>
<td>11.</td>
<td>Enter your credentials, and then click <strong>Sign In</strong>.</td>
</tr>
</tbody>
</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**.

**Note** For information on updating Subject Alternate Names (SANs), refer to *Configuration Examples and TechNotes > Unified CCE Solution: Procedure to Obtain and Upload Third-Party CA certificates*.

**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 Finesse 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 Finesse 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 Purpose** 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 Purpose** drop-down list, select **tomcat-trust**.
- b) In the **Upload File** field, click **Browse** and browse to the intermediate certificate file.
- c) Click **Upload File**.

**Step 8** Upload the application certificate.
- a) From the **Certificate Purpose** drop-down list, select **tomcat**.
- b) In the **Upload File** field, click **Browse** and browse to the application certificate file.
- c) Click **Upload File**.

**Step 9** After the upload is complete, sign out from the Platform Admin page of Finesse.

**Step 10** Access the CLI on the primary Finesse server.

**Step 11** Enter the command **utils service restart Cisco Finesse Notification Service** to restart the Cisco Finesse Notification service.

**Step 12** Enter the command **utils service restart Cisco Finesse Tomcat** to restart the Cisco Finesse 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](http://www.apple.com/mac)).

Configuring DNS on client computers allows the clients to resolve the fully-qualified domain name (FQDN) of the active Finessse 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 Finessse 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 Finessse. 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

- 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 Finess 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.

Related Topics

- Add Self-Signed Certificates for Live Data, on page 265
- Set Up Certificates for Live Data, on page 76

Add Live Data Reports to Finesses

The following sections describe how to add the Live Data reports to the Finess 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 Finess 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 Finess 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 Finess default layout XML contains commented XML code for the Live Data report gadgets available for the Finess 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 Finesses. If you upgraded Finess 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:Port Number(8445)/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 Finesses 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=99E6C8E21000014100000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB7B8E1000014100000001C50A0006C4&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 Finesses 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 Finesses default layout XML contains commented XML code for the Live Data report gadgets available for the Finesses 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=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&
viewId_2=9AB7848B100001410000001C50A0006C4&
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>
</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=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B100001410000001C50A0006C4&
```
Add Live Data Reports to Team 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 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 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:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E21000014100000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
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.

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.
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=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&
viewId_2=9AB7848B100001410000001C50A0006C4&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=99E6C8E210000141000000D80A0006C4&filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B100001410000001C50A0006C4&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:

```html
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
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=5C90012F10000140000000830A4E5B33&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**.
After you add the 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 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>
<tr>
<td>Agents cannot sign in to the desktop after a fresh installation.</td>
<td></td>
</tr>
<tr>
<td>If</td>
<td>Then</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>1. Verify that the agent ID and password are correct. <strong>Note</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>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</td>
<td><a href="">LVL::Info</a> The preceding message indicates that DNS was not configured during the installation. Reinstall Finesse and configure the DNS with a valid domain.</td>
</tr>
<tr>
<td>3. Verify that the agent is configured in Unified CCE.</td>
<td></td>
</tr>
<tr>
<td>4. Verify that the AWDB is configured correctly.</td>
<td></td>
</tr>
<tr>
<td>1. Check the realm.log for the following line: &quot;ERROR com.cisco.ccbu.finesse.realms.ccerealm.CCERealmConfig - Cannot connect to any AWDB! Ensure that at least one AWDB is configured properly and running!&quot;</td>
<td>This line indicates that Finesse cannot connect to the AWDB.</td>
</tr>
<tr>
<td>2. Check that the values entered in the Contact Center Enterprise Administration &amp; Data Server Settings gadget are correct.</td>
<td></td>
</tr>
<tr>
<td>• Verify that the username entered is a Windows domain user.</td>
<td></td>
</tr>
<tr>
<td>• Verify that the username is not prepended with the domain (for example, domain\username).</td>
<td></td>
</tr>
<tr>
<td>• Verify that the port configured is open to the Finesse server.</td>
<td></td>
</tr>
<tr>
<td>3. Check that the AWDB is set up correctly and running.</td>
<td></td>
</tr>
<tr>
<td>• The AWDB SQL server must use Windows authentication.</td>
<td></td>
</tr>
<tr>
<td>• Verify that the AWDB server is up and that the Distributor service is running.</td>
<td></td>
</tr>
<tr>
<td>5. Restart Cisco Finesse Tomcat on the primary and secondary Finesse servers.</td>
<td></td>
</tr>
<tr>
<td>6. Verify that the agent's device is properly configured in Unified</td>
<td></td>
</tr>
</tbody>
</table>
Communications Manager and is active.

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communications Manager and is active.</td>
<td></td>
</tr>
</tbody>
</table>

## Configure SQL User Account for Outbound Options High Availability

Complete these steps to configure the Microsoft SQL User for Outbound Options High Availability database operations:

### Procedure

**Step 1**
Launch Microsoft SQL Server Management Studio on the Unified CCE Administration Client workstation.

**Step 2**
Navigate to **Security > Logins**, right-click **Logins** and select **New Logins**.

You use this login when you configure the data sources for Cisco Unified Intelligence Center reporting.

**Step 3**
On the General Screen:

a) Enter the Login Name.
b) Select **SQL Server authentication**.
c) Enter and confirm the password.

**Step 4**
In the **Server Roles** page, check the **sysadmin** check box.

**Step 5**
On the User Mapping page, check the `<customer instance>_bA` and `<customer instance>_bB`.

**Step 6**
Navigate to **Security > Logins > NT AUTHORITY\SYSTEM**, right-click **Properties**.

**Step 7**
In the **Server Roles** page, check the **sysadmin** check box.

**Step 8**
Click **OK**.
CHAPTER 6

Upgrade Overview

• Multistage Upgrades and Maintenance Windows, on page 173
• Unified CCE Contact Center Upgrade Flowcharts, on page 176
• Silent Upgrade, on page 183
• Unified CCE Release 11.6(1) Upgrade Overview, on page 183

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.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Identity Service (IdS)/Single Sign-On(SSO)</td>
<td>• IdS Server</td>
<td>SSO is an optional feature and exchanges authentication and authorization details between an identity provider (IdP) and an identity service (IdS). If you upgrade to 11.6(1) from 11.5(x) with SSO enabled then upgrade the standalone Cisco IdS server before upgrading other components like Cisco Unified Intelligence Center (CUIC), and Finesse. For co-resident configurations, CUIC must be at the same version as Finesse. Upgrade both, CUIC and Finesse in the same maintenance window.</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>
<tr>
<td>1</td>
<td>Agent and supervisor desktops</td>
<td>• Cisco Finesse</td>
<td></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>Cisco Unified Intelligence Center 11.6(1) supports TLS 1.2 only. For Cisco Unified Intelligence Center 11.6(1) to be compatible with releases earlier than Unified CCE Release 11.6(1), run the CLI command <code>set client tls min-version</code>. This command allows you to set the minimum TLS version in the client for outbound SSL connections to TLS 1.0 or 1.1. Restart the system for the changes to take effect. For information about the CLI command to display the current TLS minimum version for client, see Transport Layer Security CLI Commands, on page 255.</td>
</tr>
<tr>
<td>5</td>
<td>Central Controller</td>
<td>• Unified CCE Router • Unified CCE Logger • Admin &amp; Data server (AW/HDS/DDS) • Standalone Live Data (if Deployed) • CUIC Reporting Templates • CCMP • Administration Client</td>
<td></td>
</tr>
</tbody>
</table>
### Upgrade Overview

#### Multistage Upgrades and Maintenance Windows

<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Peripherals</td>
<td>• Agent (Unified Communications Manager) PG or System PG, plus • CTI Server • CTI OS Server • Outbound Option Dialer and SIP IOS Gateway • VRU PG (if collocated with Agent PG on VM) • MR PG (if collocated with Agent PG on VM), plus • Unified CCE Gateway PG (if collocated with Agent PG on VM)</td>
<td>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.</td>
</tr>
<tr>
<td>7</td>
<td>Peripherals</td>
<td>• MR PG (if not collocated with Agent PG on VM), plus • VRU PG (if not collocated with Agent PG on VM) • Unified CCE Gateway PG (if not collocated with Agent PG on VM) • CRM connector</td>
<td>You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window.</td>
</tr>
<tr>
<td>8</td>
<td>Agent desktop client software</td>
<td>• CTI OS (Agent/Supervisor Desktops)</td>
<td>You can have many desktops located in many different sites. You can upgrade CTI OS desktops in multiple maintenance windows; the later upgrade stages are not dependent on the completion of this stage.</td>
</tr>
</tbody>
</table>

---

**Agent desktop client software**

Recursive, see Notes
<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 9     | Call Processing   | • Cisco Unified Communications Manager (Unified Communications Manager)  
        |                   | • JTAPI on Agent (Unified Communications Manager) PG            | MediaSense is a standalone application that you can upgrade at any time after IOS Gateway upgrades.³ |
| Any (See Notes) | Media Recording  | • MediaSense                                                | MediaSense is a standalone application that you can upgrade at any time after IOS Gateway upgrades.³ |

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

³ UCCE 11.6(1) supports only Cisco MediaSense 11.5.

**Unified CCE Contact Center Upgrade Flowcharts**

The following diagram illustrates the solution-level upgrade flow for a Cisco Unified Contact Center Enterprise solution upgrade.
Upgrade Overview

Stage 0
Identity Service (IdS) / Single Sign-On (SSO)
- IdS Server

Stage 1
Agent and Supervisor Desktops
- ECE, Finesse

Stage 2
Queuing and self-service
- CVP (Operations Console, Reporting Server, Call Server/XMLServer, Unified Call Studio)

Stage 3
Gateways
- Voice and Data Gateways

Stage 4
Reporting Management
- CUIC (Reporting Server)
- For co-resident deployment (CUIC-LD-IDS)
  complete Stage 4 at the same time as Stage 5

Stage 5
Unified CCE Central Controller
- Unified CCE Router
- Unified CCE Logger
- AW/HDS/DDS
- CUIC (Reporting Templates)
- Live Data
- CCMP
- Administration Client

Stage 6
Collocated Peripheral Gateways and associated components
- Agent PG/System PG
  - Outbound Option Dialer and SIP IOS Gateway
  - CTI Server
  - CTI OS Server
  (if using system PG)
  - Remote Silent Monitor
- VRU PG (if collocated with Agent PG/System PG)
- MR PG (if collocated with Agent PG/System PG)
- Unified CCE Gateway PG (if collocated with Agent PG/System PG)

Stage 7
Peripheral Gateways and associated components not collocated
- VRU PG
- MR PG
- Unified CCE Gateway PG

Stage 8
Agent and Supervisor Desktops
- CTI OS Desktops (if using system PG)

Stage 9
Call Processing
- Unified Communications Manager
- Upgrade JTAPI on Agent PG

Stage 10
Media Recording
- MediaSense

End
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

C

Upgrade CUIC Reporting Server

Live Data
(if standalone)

Technology Refresh or
Common Ground

Common Ground
Technology Refresh

D

Obtain licenses for the release

Back up server registry, databases

New domain?

yes

no

Migrate Active Directory and DNS to non-UnifiedCCE servers

Export Active Directory users

Temp A&D servers required for continuity of configuration and reporting?

yes

no

Set up temp A&D servers

Disable configuration changes

F
Upgrade Overview

Unified CCE Contact Center Upgrade Flowcharts

1. Obtain licenses for this release
2. Back up server registry, databases
3. Disable configuration changes
4. Export server registry
5. Migrate Active Directory and DNS to non-UnifiedCCE servers
   - yes: New domain?
   - no: Temp A&D servers required for continuity of configuration and reporting?
   - yes: Set up temp A&D servers
   - no: Export Active Directory users

F
Silent Upgrade

There are situations where a silent upgrade can be used in running an installation wizard. You can run a silent installation when performing a fresh install or an upgrade.

For information, see the section on silent installation.

Related Topics

Silent installation, on page 57

Unified CCE Release 11.6(1) Upgrade Overview

Before you upgrade to Unified CCE Release 11.6(1), ensure that Unified CCE Release 11.x is installed on your machine. If you use Unified CCE Release 10.0(x) or Release 10.5(x), first upgrade to Unified CCE Release 11.0(1) using 11.0 ICM-CCE-CCH Installer.

The supported upgrade paths to 11.6(1) are as follows:

- Release 10.0(x) to Release 11.0(1), followed by 11.6(1)
- Release 10.5(x) to Release 11.0(1), followed by 11.6(1)
- Release 11.0(1) to 11.6(1)
- Release 11.0(2) to 11.6(1)
- Release 11.5(1) to 11.6(1)

Note

Any other Maintenance Release on 11.x needs to be removed before upgrading to 11.6(1). It may also be possible to upgrade directly to a Maintenance Release on top of 11.6(1) from other MR not mentioned in the above list.

For more information on available MR, see https://software.cisco.com/download/release.html?mdfid=268439622&flowid=46046&softwareid=280840583


For more information on the uninstallation process, see the section Uninstall Methods, on page 237.

Note

As CCE 11.6 enforces the use of TLS 1.2 in the entire solution, an upgrade to SQL Server 2014 SP2 is a prerequisite before upgrading to 11.6(1).

Related Topics

Transport Layer Security Version 1.2 Required, on page 4
Upgrade to Unified CCE Release 11.6(1)

Before you begin

• An upgrade to Release 11.6(1) requires Windows Update KB2919355 (Hotfix). If you applied a Windows update since March 2014, this update should be installed. To determine if this Windows Hotfix is installed, from your Control Panel go to Programs > Programs and Features. Click View installed updates. Make sure that Windows Update is not running in parallel when you install the Release 11.6(1) patch.

• Before upgrading Unified CCE, update the OS and SQL Server on your VMs to meet the requirements listed on the Unified CCE Solution Compatibility Matrix. Your upgrade can fail if the OS and SQL Server versions do not meet these requirements.

• Database partitioning, if enabled, prevents Unified CCE Release 11.6(1) upgrade because database partitioning was obsoleted in Unified CCE Release 9.0(1). Remove partitioning before you run the Unified CCE Release11.6(1) installer.

To remove partitioning from logger/AW/HDS database, follow the steps mentioned in the tech-zone article: https://techzone.cisco.com/t5/Administration-and-Data-Servers/Removing-Database-partitioning-UCCE-8-5-4/ta-p/743317.

• The minimum disk space required to perform the upgrade is 2175 MB.

• During the upgrade process, the installer takes a backup of the existing configuration database. This backup is available in drive\temp\<instance name_logger side><Major_CC_Minor_AW_Minor>

Note The values for Major, CCMajor, AWMinor that are used in the backup folder name, are derived from the 11.0 or 11.5 schema version of the system being upgraded (These are stored in the Version table of the CCE database and would translate into 181,3,3 for upgrades from 11.0(x) systems and 188,0,0 for 11.5(x) upgrades).

For example: C:\Temp\Inst_sideA_181_3_3 from 11.0(1) upgrade and C:\Temp\Inst_sideA_188_0_0 from 11.0(1) upgrade

Note: This backup may fail if the space required to backup configuration data as calculated by the installer is not available on the system. This is independent of the minimum space requirement listed above.

• Before upgrading or uninstalling 11.6(1) Installer, close all the open Windows Event Viewer instances. If you do not follow the same, the installer may fail to proceed. You might see an error that says the following DLLS are locked.

  • icrcat.dll
  • icrmsgs.dll
  • snmpeventcats.dll
• snmpeventmsgs.dll

In such a scenario, close the Event Viewer and retry the installation or uninstallation.

Procedure

Step 1 Log in to your system as a user with administrative privileges.
Step 2 After either downloading the installer or placing the media in the drive, start the Cisco ICM Minor Release ICM 11.6(1) Installer.
Step 3 Follow the on-screen instructions to install Unified CCE Release 11.6(1).

Note A pop-up window displays a notification that some services were automatically changed to Manual as part of the upgrade. Make sure that both A and B sides of your system operate properly after the Unified CCE Release 11.6(1) upgrade. Then, set the ICM services that were changed during the upgrade back to their original setting (Automatic).

If you are not sure which services were changed from Automatic to Manual during the upgrade, examine the setup logs located in C:\Temp\Minor Release ICM11.6(1).

Step 4 If you use the Diagnostic Portal to monitor Live Data standalone servers, rerun the following command:

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

Related Topics

Configure Live Data Machine Services, on page 75
Common Ground Upgrade

- Preupgrade Overview, on page 187
- Common Ground Preupgrade Task Flow, on page 188
- Common Ground Preupgrade Tasks, on page 189
- Common Ground Upgrade Task Flow, on page 193
- Common Ground Upgrade Tasks, on page 197

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.

Custom Region Fix Tool

You must run the mandatory CustomRegionFixTool before upgrading to Release 11.6 to avoid any region data corruption.

CustomRegionFixTool.exe:

Before upgrading Unified CCE, run the CustomRegionFixTool.exe tool on machines that have <inst_sideA>, <inst_sideB>, and <inst_awdb> databases.

You can download CustomRegionFixTool.exe from Cisco.com.

Upgrade 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.

• Upgrade.exe—Used to upgrade the schema of the logger, AW DB, HDS DB, and BA databases to a version compatible with the current CCE Software version. It is typically used when the installer fails to automatically upgrade the schema.

Perform the following steps to use the tool:

<Install Drive>: \icm\bin>upgrade.exe -s <Server Name> -d <Database name> -dt <Database Type> -i <Instance Name>

Where

(Database Type) - can be either "logger" or "hds" or "aw" or "ba", depending on the database that requires the schema to be upgraded.

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>Release 10.5 to 11.0</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi Supportability</td>
<td>yes</td>
<td></td>
<td>ESXi Supportability, on page 7</td>
</tr>
<tr>
<td>Disaster Recovery Plan</td>
<td>yes</td>
<td></td>
<td>Disaster Recovery Plan, on page 190</td>
</tr>
<tr>
<td>Change the SCSI Controller Type</td>
<td>yes</td>
<td></td>
<td>Change the SCSI Controller Type, on page 190</td>
</tr>
<tr>
<td>Upgrade VM Network Adapters from E1000 to VMXNet3</td>
<td>yes</td>
<td></td>
<td>Upgrade VM Network Adapters from E1000 to VMXNet3, on page 191</td>
</tr>
<tr>
<td>VM Hardware Version Upgrade</td>
<td>yes</td>
<td></td>
<td>VM Hardware Version Upgrade, on page 192</td>
</tr>
<tr>
<td>Download the Enhanced Database Migration Tool</td>
<td>yes</td>
<td></td>
<td>Upgrade Overview</td>
</tr>
</tbody>
</table>
### Common Ground Preupgrade Tasks

#### Disable configuration changes

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>To disable configuration changes during the upgrade, set the following registry key to 1 on the Side A Call Router: <code>HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\ICM\&lt;instance name&gt;\Router\A\Router\CurrentVersion\Configuration\Global\DBMaintenance</code>.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Confirm that configuration changes are disabled by attempting to save a configuration change.</td>
</tr>
</tbody>
</table>
When you try to save the change, a message is displayed confirming the change failure.

---

**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**

**Step 1** Ensure the virtual machine is powered on.

**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.

**Step 6** Log in to the virtual machine.

The operating system automatically detects the new SCSI controller and adds the driver for LSI Logic SAS.

**Step 7** In Device Manager, under Storage controllers, ensure that the controller is listed as LSI Adapter SAS 3000 Series.

**Step 8** Power down the virtual machine.

**Step 9** 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.

**Step 11** Power on the virtual machine.
Step 12 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.

---


---

**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.
Increase the Provisioned Disk Size for Unified Intelligence Center VMs (Standalone and Coresident)

Procedure

Step 1  Power off the virtual machine.
Step 2  Click Edit Settings.
Step 3  Click the Hardware tab, and select the hard disk to modify.
Step 4  In the Disk Provisioning pane, increase the provisioned size from 146 GB to 200 GB.
Step 5  Click OK to save your changes and close the dialog box.
Step 6  Start the virtual machine.

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>Infrastructure and media resource</td>
<td></td>
</tr>
<tr>
<td>components</td>
<td>* Upgrade voice and data gateways. <a href="#">Upgrade Voice and Data Gateways, on page 207</a></td>
</tr>
<tr>
<td>Reporting server</td>
<td></td>
</tr>
</tbody>
</table>
### Task

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
</table>
| Upgrade Cisco Unified Intelligence Center server.                    | *Installation and Upgrade Guide for Cisco Unified Intelligence Center at*

### Unified CCE Central Controller and Administration & Data Server components

| Bring down Side A Logger, and upgrade the VM to the new platform of Windows Server and SQL Server. | Upgrade to Windows Server 2012 R2, on page 197 |
| Bring down Side A Call Router, and upgrade the VM to new platform of Windows Server. | Upgrade to Windows Server 2012 R2, on page 197 |
| Upgrade Side A Call Router. | Upgrade Unified CCE Call Router, on page 202 |
| Upgrade the VM for the Administration & Data Server connected to Side A to the new platform of Windows Server and SQL Server. | Upgrade to Windows Server 2012 R2, on page 197 |
| Upgrade the Administration & Data Server connected to Side A. | Migrate HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 202 |

*Common Ground Upgrade Task Flow*
<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<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 207</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 197</td>
</tr>
<tr>
<td></td>
<td>Upgrade to SQL Server 2014, on page 200</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 201</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 197</td>
</tr>
<tr>
<td>Upgrade Side B Call Router.</td>
<td>Upgrade Unified CCE Call Router, on page 202</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 209</td>
</tr>
<tr>
<td>Bring Side B Logger into service and verify operation.</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Upgrade the VM for the Administration & Data Server connected to Side B to the new platform of Windows Server and SQL Server. | Upgrade to Windows Server 2012 R2, on page 197  
Upgrade to SQL Server 2014, on page 200                                                                 |
| Upgrade the Administration & Data Server connected to Side B.       | Migrate HDS Database and Upgrade the Unified CCE Administration & Data Server, on page 202                                     |
| Upgrade Cisco Unified Intelligence Center reporting templates.       | *Installation and Upgrade Guide for Cisco Unified Intelligence Center* at  
| Upgrade Unified Contact Center Management Portal(Unified CCMP).     | *Installation and Configuration Guide for Cisco Unified Contact Center Management Portal* at  
| Upgrade Administration Client.                                      | Upgrade Unified CCE Administration Client, on page 228                                                                            |
| Database Performance Enhancement.                                    | Database Performance Enhancement, on page 212                                                                                     |
| **Unified CCE Peripheral Gateways and associated components**       |                                                                                                                                 |
| Upgrade PGs to new platform of Windows Server.                      | Upgrade to Windows Server 2012 R2, on page 197                                                                                     |
| Upgrade PGs.                                                        | Upgrade Peripheral Gateways, on page 203                                                                                           |
| Upgrade Outbound Option Dialer.                                     | Upgrade Outbound Option Dialer, on page 204                                                                                         |
| Upgrade CTI server.                                                 | *CTI OS System Manager Guide for Cisco Unified ICM/Contact Center Enterprise* at  
### 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, for example Finesse and CUIC, see the links to component-specific documents in the Common Ground Upgrade Task Flow, on page 193.

### 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.
Unified CCE 11.0(x) supports only Windows Server 2012 R2. 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

- 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 190.

- 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 191.

- 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 191.

- In the vSphere Client, ensure that you have upgraded the VM hardware version to the version 9 see VM Hardware Version Upgrade, on page 192.

- 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 199.
- Multilingual language pack will be uninstalled. Install the language pack manually. For more information on installing language pack, see Microsoft documentation at http://www.microsoft.com/OEM/en/installation/downloads/Pages/Windows-Server-2012-Language-Packs.aspx#fbid=bSYXlh5sO3X.
- Check the persistent static routes and static network configurations (for private and public interfaces). If the network settings are lost, reconfigure it manually.

Related Topics
- Change the SCSI Controller Type, on page 190
- Set Up Virtual Machines, on page 16
- Technology Refresh Upgrades, on page 2
- Upgrade VM Network Adapters from E1000 to VMXNet3, on page 191

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

Step 1 Click Start, search disk cleanup and then click Disk Cleanup.
Step 2 In the Disk Cleanup Options dialog box, click Files from all users on this computer.
Step 3 In the User Account Control dialog box, click Continue.
Step 4  Click to select the previous Windows Installation check box, and then click OK.

---

**Upgrade to SQL Server 2014**

Microsoft supports in-place upgrade of operating system and SQL Server. After you upgrade the operating system, upgrade to SQL Server 2014.

---

**Note**


---

**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 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.
- if you use Outbound option, migrate the outbound option database.
- Install the new software.

### 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

**Step 1**

Using Unified CCE Service Control, stop all Unified CCE services on the Server and change to Manual Start.

**Step 2**

Launch the EDMT, and click **Next**.

**Step 3**

Select **Common Ground**, and click **Next**.

**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.

**Step 5**

In the Database Connection section, highlight the database that you want to upgrade, and then click **Next**.

**Step 6**

Click **Start Migration**. A warning message is displayed asking for confirmation of the data migration.

**Step 7**

Click **Yes** to confirm.

**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.

**Step 9**

Exit the EDMT.

If Outbound Option is deployed, repeat the same steps to migrate the BA database.
**Upgrade Unified CCE Call Router**

**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 197.

**Procedure**

- **Step 1**: Reboot the Call Router virtual machine.
- **Step 2**: Launch the 11.0 ICM-CCE-Installer and click **Next**.
- **Step 3**: (Optional) To apply any Minor Releases, click **Browse** and navigate to the Minor 11.6(1) 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-Installer 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 11.0 ICM-CCE-Installer and click Next.

Step 4 Optional: To apply any Minor Releases, click Browse and navigate to the 11.6(1) Minor 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.

Related Topics
Upgrade to SQL Server 2014, on page 200
Upgrade to Windows Server 2012 R2, on page 197

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 CTIOS component, upgrade the CTIOS 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 197.

Procedure

Step 1 Launch the 11.0 ICM-CCE-CCHInstaller and click Next.
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 11.0 ICM-CCE-Installer and click Next.
Step 2 (Optional) To apply any Minor Releases, click Browse and navigate to the 11.6(1) Minor 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 11.0 AdminClientInstaller and click Next.
Step 2 (Optional) To apply any Minor Releases, click Browse, and navigate to the 11.6(1) Minor 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.
Enable Configuration Changes

Procedure

**Step 1**
To enable configuration changes during the upgrade, set the following registry key to 0 on the Side A Call Router: `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\ICM\<instance name>\Router\Router\CurrentVersion\Configuration\Global\DBMaintenance`.

**Step 2**
Confirm that configuration changes are enabled by attempting to save a configuration change. Save your changes.
Common Upgrade Tasks

- Upgrade Voice and Data Gateways, on page 207
- Bring upgraded Side A into service, on page 207
- Verify operation of upgraded Side B Call Router and Logger, on page 209
- Upgrade Cisco JTAPI Client on the Unified Communications Manager PG, on page 211
- Database Performance Enhancement, on page 212

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>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>

5 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:
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-Installer 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>
</tbody>
</table>
Verify operation of upgraded Side B Call Router and Logger

### 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>
</table>
| Loggers                       | • Logger: Connected to its respective database and synchronized with peer. MDS is in service.  
                               | • Replication: No connectivity to Administration & Data Server HDS at this time. |
| Call Routers                  | • Router: Running and synchronized with peer.               |
|                               | • Ccagent: In service but not connected to any peripheral gateways. |
|                               | • Rtsvr: Feed activated to Administration & Data Server.    |
| Loggers                       | • Logger: Connected to its respective database and synchronized with peer. MDS is in service.  
                               | • Replication: Connected to the Administration & Data Server. |
| Administration & Data Server  | • Updateaw: Displays "Waiting for new work."               |
|                               | • Iseman: Listen thread waiting for client connection. (Exists only if Internet Script Editor is configured.) |
|                               | • Replication: Replication and recovery client connection initialized.  

**Note** 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:

```
\%\w%ICM<instancename>\Distributor\RealTimeDistributor\ClientVersion\Recovery\ClientVersion\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\<instance name>\Router\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 225.

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, restart the server, and reinstall a new version. You install the JTAPI client using the Unified Communications Manager Administration application.

Before you begin
Before you perform this procedure, you must:

   • Uninstall the old JTAPI client from the Unified Communications Manager PG
   • Restart the PG server.

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 link next to Download Cisco JTAPI for Windows. Download the 32 bit version only.

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, complete the following procedure 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Use the Unified CCE Service Control to stop the Logger service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the command prompt, run the RunFF.bat file which is located in the &lt;SystemDrive&gt;:\icm\bin directory.</td>
</tr>
</tbody>
</table>
| 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Use the Unified CCE Service Control to stop the Distributor service.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the command prompt, run the RunFF.bat file which is located in the &lt;SystemDrive&gt;:\icm\bin directory.</td>
</tr>
</tbody>
</table>
| 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.
Improve Reporting Performance

To improve the performance of the reporting application, modify the following Windows settings on the database servers (AW-HDS, AW-HDS-DDS, HDS-DDS).

- Increase the Paging File Size to 1.5 times the server’s memory.

  To change the Paging File Size, from the Control Panel search for Virtual Memory. In the Virtual Memory dialog box, select **Custom size**. Set both **Initial size** and **Maximum size** to 1.5 times the server memory.

- Set the server’s **Power Options** to **High Performance**.

  From the Control Panel, select **Power Options**. By default, the **Balanced** plan is selected. Select **Show additional plans** and select **High performance**.

In SQL Server, disable **Auto Update Statistics** for AW and HDS databases.

In the SQL Server Management Studio, right-click the database name in the Object Explorer and select **Properties**. Select the **Options** page. In the **Automatic** section of the page, set **Auto Create Statistics** and **Auto Update Statistics** to **False**.
Common Upgrade Tasks

Improve Reporting Performance
Technology Refresh Upgrade

- Preupgrade Overview, on page 215
- Technology Refresh Preupgrade Task flow, on page 216
- Upgrade Overview, on page 217
- Technology Refresh Upgrade Task Flow, on page 219
- Technology Refresh Upgrade Tasks, on page 223

**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.

**Custom Region Fix Tool**

You must run the mandatory CustomRegionFixTool before upgrading to Release 11.6 to avoid any region data corruption.

CustomRegionFixTool.exe:

Before upgrading Unified CCE, run the CustomRegionFixTool.exe tool on machines that have `<inst_sideA>`, `<inst_sideB>`, and `<inst_awdb>` databases.

You can download CustomRegionFixTool.exe from Cisco.com.

**Upgrade 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.

• Upgrade.exe—Used to upgrade the schema of the logger, AW DB, HDS DB, and BA databases to a version compatible with the current CCE Software version. It is typically used when the installer fails to automatically upgrade the schema.

Perform the following steps to use the tool:

<Install Drive>: \icm\bin>upgrade.exe -s <Server Name> -d <Database name> -dt <Database Type> -i <Instance Name>

Where

<Database Type> - can be either "logger" or "hds" or "aw" or "ba", depending on the database that requires the schema to be upgraded.

Technology Refresh Preupgrade Task flow

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 Router: 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 Contact Center Enterprise at [https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html) 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.
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, Check the Virtualization for Unified Contact Center Enterprise at https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-unified-contact-center-enterprise.html for descriptions of each OVA.

**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:

- **11.0(1) 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.

  Optionally, 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 55.

- **Note**

  Optionally, update the Apache Tomcat software. See *Upgrade Tomcat*, on page 56.

  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.
  - 11.0(1) 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.
  - ICM11.6(1).exe Installer - The Minor Release 11.6(1) installer which needs to be applied on 11.x base version.
  - 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](https://www.cisco.com).

**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.

**Note**
User Migration Tool cannot be used for migrating users that are SSO enabled.

- 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.

## 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>Agent and supervisor desktops</td>
<td></td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>------</td>
<td>-----</td>
</tr>
</tbody>
</table>

**Queuing and self-service components**

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

**Infrastructure and media resource components**

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade voice and data gateways</td>
<td>Upgrade Voice and Data Gateways, on page 207</td>
</tr>
</tbody>
</table>

**Reporting server**

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

**Unified CCE Central Controller and Administration & Data Server components**

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<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 223</td>
</tr>
<tr>
<td>Bring down Side A Call Router, and upgrade</td>
<td>Upgrade Unified CCE Call Router, on page 224</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 225</td>
</tr>
<tr>
<td>Task</td>
<td>See</td>
</tr>
<tr>
<td>------</td>
<td>-----</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 207</td>
</tr>
<tr>
<td>Migrate Side B Logger database and upgrade Logger</td>
<td>Migrate the Logger Database and Upgrade the Logger, on page 223</td>
</tr>
<tr>
<td>Upgrade Side B Call Router</td>
<td>Upgrade Unified CCE Call Router, on page 224</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 209</td>
</tr>
<tr>
<td>Bring Side B Logger into service and verify operation.</td>
<td>Migrate HDS Database and Upgrade Unified CCE Administration &amp; Data Server, on page 225</td>
</tr>
</tbody>
</table>
## Technology Refresh Upgrade Task Flow

<table>
<thead>
<tr>
<th>Task</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Administration Client</td>
<td>Upgrade Unified CCE Administration Client, on page 204</td>
</tr>
<tr>
<td>Database Performance Enhancement</td>
<td>Database Performance Enhancement, on page 212</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 227</td>
</tr>
<tr>
<td>Upgrade Outbound Option Dialer</td>
<td>Upgrade Outbound Option Dialer, on page 228</td>
</tr>
<tr>
<td><strong>Desktop Client components</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Call Processing components</strong></td>
<td></td>
</tr>
<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 211</td>
</tr>
<tr>
<td><strong>Media Recording components</strong></td>
<td></td>
</tr>
</tbody>
</table>

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

7 UCCE 11.6(1) supports only Cisco MediaSense 11.5.
### 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.

### Migrate the Logger Database and Upgrade the Logger

To upgrade the Logger, you do the following tasks:

- Migrate the Logger database.
- If you use Outbound option, migrate the outbound option database.
- Install the new software.

#### 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* check box is checked.
- In the Properties window > Security tab, the permission level is set as full control for everyone.

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Use Unified CCE Service Control to stop all Unified CCE services on the Logger.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Run the EDMT from the server that hosts the destination Logger and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <em>Technology Refresh</em> and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Under <em>Source Database Connection</em>, in the <em>HostName\IPAddress</em> field, type the Source IP and click <em>Refresh Database List</em>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select the Logger Database name, and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Windows Share Name field, type the name of the shared folder that you created.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Windows Share Password field, type the password of the destination machine, and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Review or change the information displayed as required and click <em>Start Migration</em>.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Exit the EDMT.</td>
</tr>
<tr>
<td>Step 10</td>
<td>If Outbound Option is deployed, to migrate the BaA database, reopen the EDMT and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 11</td>
<td>Select <em>Technology Refresh</em> and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 12</td>
<td>Under <em>Source Database Connection</em>, in the <em>HostName\IPAddress</em> field, type the Source IP and click <em>Refresh Database List</em>.</td>
</tr>
<tr>
<td>Step 13</td>
<td>Select the Outbound Database name, and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 14</td>
<td>In the Windows Share Name field, type the name of the shared folder that you created.</td>
</tr>
<tr>
<td>Step 15</td>
<td>In the Windows Share Password field, type the password of the destination machine, and click <em>Next</em>.</td>
</tr>
<tr>
<td>Step 16</td>
<td>Review or change the information displayed as required and click <em>Start Migration</em>.</td>
</tr>
<tr>
<td>Step 17</td>
<td>Exit the EDMT.</td>
</tr>
</tbody>
</table>
Step 18 Launch the ICM-CCE-Installer 11.0(1) 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 11.6(1) Minor Releases, click Browse and navigate to the Minor 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 187.
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-Installer and click Next.
Step 2
Step 3 (Optional) To apply any 11.6(1) Minor Release or Maintenance Releases, click Browse and navigate to the Maintenance or Minor 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 server when the upgrade completes.
Step 9  Open the Web Setup tool from the Installer dialog box or desktop shortcut.
Step 10 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 11 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 12 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 Migrate HDS Database and Upgrade Unified CCE Administration & Data Server, on page 225.
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 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-Installer 11.0(1) and click Next.

Step 11  (Optional) To apply any Minor Releases or other Maintenance Releases, click Browse and navigate to the Minor 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.

---

**Synchronizing or Updating Data from Logger or HDS Production Server to Staged 11.6(1) Server During Cut-over**

The EDMT tool can also be used to migrate data from a Logger or HDS production server, to the one that has already been staged on version 11.6(1). These two pronged upgrade steps are typically performed to reduce the downtime needed during cut-over to the new version.

While the parallel 11.6(1) systems are staged and tested, the 10.x production servers continue to process calls. On the day of the cut-over, the data in the 11.6(1) staged servers, can be updated or synchronized with that of the production server, by running the EDMT tool, for each of the Logger and HDS database.

**Note**  Stop the Logger, AW-HDS, and Apache Tomcat services on 11.6 staged systems, before running EDMT tool while changing over to synchronize.
However, due to the 11.6(1) database schema version (188, 1, and 1) being different from its base 11.0 version (181, 3, and 3), the synchronized database will be incompatible with 11.6(1). The administrator would have to manually use upgrade.exe utility to upgrade the database schema before starting the CCE Logger or Distributor service.

The utility is present in the icm\bin folder, and needs to be run against each of the database that was updated / synchronized from the production server.

Perform the following steps to use the tool:

<Install Drive>: \icm\bin>upgrade.exe -s <Server Name> -d <Database name> -dt <Database Type> -i <Instance Name>

Where

<Database Type> - can be either "logger" or "hds", depending on the database that requires the schema to be upgraded.

For Example C:\icm\bin>upgrade -s PRGR-A -d abc_sideA -dt logger -i abc

# - The value as stored in columns Major,CCMinor, and AWMinor of Version table in the CCE database.

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 CTIOS component, upgrade the CTIOS 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

Step 1 Use Unified CCE Service Control to stop all Unified CCE and CTIOS (if applicable when upgrading the Unified Communications Manager PG) services on the PG server. Change the services to Manual Start.

Step 2 Launch the ICM-CCE-Installer and click Next.

Step 3 (Optional) To apply any 11.6(1) Minor Releases or other 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.

The registry information for the Unified Communications Manager PG also contains information for the CTIOS server (if applicable).

Step 6 Click OK on any informational messages that display.

Step 7 Click Install.
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 Outbound option database during the 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-Installer 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 223

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
CHAPTER 10

Upgrade from a Standalone Deployment to a Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

- Upgrade from a Standalone to a Co-resident Deployment, on page 229
- Set Deployment Type in Unified CCE Administration Configuration, on page 229
- Install and Upgrade COP File, on page 230
- Install Publisher/Primary Nodes of VOS-Based Contact Center Applications, on page 230
- Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 232
- Set Up the System Inventory, on page 234
- Install Vmware Tools, on page 234
- Configure Live Data with AW, on page 234
- Configure Live Data Unified Intelligence Center Data Sources, on page 235
- Restart Live Data, on page 236

Upgrade from a Standalone to a Co-resident Deployment

Release 11.6(1) adds a new deployment type called UCCE: 2000 Agents Rogger, that should be set for such deployments. The reference VM layout uses oversubscription to minimize the required ESXi hosts. If you have an existing standalone deployment and want to transition to the co-resident layout, then this upgrade is essential.

Set Deployment Type in Unified CCE Administration Configuration

Ensure that the deployment type has been set to UCCE: 2000 Agents Rogger via CCE Web Administration tool.

Perform the following steps to set the deployment:
Install and Upgrade COP File

Before upgrading CUIC standalone deployment to a coresident UCCE:2000 Agents deployment (CUIC with Live Data and IdS), perform the following steps:

Procedure

Step 1 Install the COP file:

- To upgrade from UCCE 10.5 to 11.6(1):
  1. Apply RU COP "ciscocuic.refresh_upgrade_v1.4.cop.sgn" on CUIC
  2. Upgrade CUIC 10.5 to CUIC 11.0(1)
  3. In case of "UCCE 2000 Agents Rogger model, install co-resident deployment COP "ciscocuic.cce2k-cores-deployment.cop.sgn" on CUIC VM to get the benefits of Coresident of CUIC, LD and IDS.
  4. Upgrade CUIC 11.0(1) to CUIC 11.6(1)

- To upgrade from UCCE 11.0(1) to 11.6(1):
  1. In case of "UCCE 2000 Agents Rogger model, install co-resident deployment COP "ciscocuic.cce2k-cores-deployment.cop.sgn" on CUIC to get the benefits of Coresident of CUIC, LD and IDS.
  2. Upgrade CUIC 11.0(1) to CUIC 11.6(1)


Step 2 Delete the standalone Live Data virtual machine after you have upgraded the standalone deployment to a coresident deployment.
Before you begin

DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Virtualized Voice Browser, Cisco MediaSense, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Note

If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create a virtual machine for your VOS-based contact center application using the OVA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Mount the ISO image for the software to the virtual machine.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select the virtual machine, power it on, and open the console.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Follow the Install wizard, making selections as follows:</td>
</tr>
<tr>
<td>a)</td>
<td>In the Disk Found screen, click OK to begin the verification of the media integrity.</td>
</tr>
<tr>
<td>b)</td>
<td>In the Success screen, select OK.</td>
</tr>
<tr>
<td>c)</td>
<td>In the Product Deployment Selection screen:</td>
</tr>
<tr>
<td>i)</td>
<td>• For the Progger (Lab only) or 2000 agent reference design, choose the coresident deployment option Cisco Unified Intelligence Center with Live Data and IdS, and then select OK. The Cisco Unified Intelligence Center with Live Data and IdS option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.</td>
</tr>
<tr>
<td>i)</td>
<td>• For all other deployments, select one of the standalone install options. For example, select Cisco Unified Intelligence Center, Live Data, or Cisco Identity Service (IdS). Then select OK.</td>
</tr>
<tr>
<td>d)</td>
<td>In the Proceed with Install screen, select Yes.</td>
</tr>
<tr>
<td>e)</td>
<td>In the Platform Installation Wizard screen, select Proceed.</td>
</tr>
<tr>
<td>f)</td>
<td>In the Apply Patch screen, select No.</td>
</tr>
<tr>
<td>g)</td>
<td>In the Basic Install screen, select Continue.</td>
</tr>
<tr>
<td>h)</td>
<td>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.</td>
</tr>
<tr>
<td>Note</td>
<td>For Live Data servers, use the same timezone for all the nodes.</td>
</tr>
<tr>
<td>i)</td>
<td>In the Auto Negotiation Configuration screen, select Continue.</td>
</tr>
<tr>
<td>j)</td>
<td>In the MTU Configuration screen, select No to keep the default setting for Maximum Transmission Units.</td>
</tr>
<tr>
<td>k)</td>
<td>In the DHCP Configuration screen, select No.</td>
</tr>
<tr>
<td>l)</td>
<td>In the Static Network Configuration screen, enter static configuration values. Select OK.</td>
</tr>
<tr>
<td>m)</td>
<td>In the DNS Client Configuration screen, click Yes to enable DNS client.</td>
</tr>
<tr>
<td>n)</td>
<td>Enter your DNS client configuration. Select OK.</td>
</tr>
<tr>
<td>o)</td>
<td>In the Administrator Login Configuration screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select OK.</td>
</tr>
<tr>
<td>p)</td>
<td>In the Certificate Information screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select OK.</td>
</tr>
</tbody>
</table>
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.
v) In the Platform Configuration Confirmation screen, select OK. The installation begins and runs unattended.
   • There is a reboot in the middle of the installation.
   • The installation ends at a sign-in prompt.

Step 5 Unmount the ISO image.

---

Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications

Before you begin
DNS Configuration is mandatory for installation of Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Virtualized Voice Browser, Cisco MediaSense, and Cisco Finesse. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Note
If the deployment uses host files in addition to DNS, use FQDNs in the host file. Live Data and single sign-on (SSO) require FQDNs to work properly.

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters.

Procedure

Step 1 Create a virtual machine for your VOS-based contact center application using the OVA.
Step 2 Mount the ISO image for the software to the virtual machine.
Step 3 Select the virtual machine and power it on.
Step 4 Follow the Install wizard, making selections as follows:
   a) In the Disk Found screen, click OK to begin the verification of the media integrity.
   b) In the Success screen, select OK.
   c) In the Product Deployment Selection screen:
      • For the Progger (Lab only) or 2000 agent reference design, choose the coreident deployment option Cisco Unified Intelligence Center with Live Data and IdS, and then select OK. The Cisco Unified
Intelligence Center with Live Data and IdS option installs Cisco Unified Intelligence Center, Live Data, and Cisco Identity Service (IdS) on the same server.

- For all other deployments, select one of the standalone install options. For example, select Cisco Unified Intelligence Center, Live Data, or Cisco Identity Service (IdS). Then select OK.

**Step 5** Follow the Install wizard, making selections as follows:

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

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

c) In the Apply Patch screen, select No.

d) In the Basic Install screen, select Continue.

e) 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.

   **Note** For Live Data servers, use the same timezone for all the nodes.

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

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

h) In the DHCP Configuration screen, select No.

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

j) In the DNS Client Configuration screen, enter your DNS client configuration. Select OK.

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

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

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

n) In the warning screen, select OK.

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

p) 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.

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

r) In the Platform Configuration Confirmation screen, select OK. The installation begins and runs unattended.

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

   - The installation ends at a sign-in prompt.

**Step 6** Unmount the ISO image.
Set Up the System Inventory

Procedure

**Step 1** In Unified CCE Administration, navigate to **System > Deployment**.

**Step 2** Add the new machine to the System Inventory:

a) Click **New**.

   The **Add Machine** popup window opens.

b) From the Type drop-down menu, select the following machine type:

   CUIC_LD_IdS Publisher, for the coresident Unified Intelligence Center, Live Data, and Identity Service machine available in the 2000 agent reference design.

c) In the **Address** field, enter the FQDN or IP address of the machine.

d) Enter the machine's Administration credentials.

e) Click **Save**.

The machine and its related Subscriber or Secondary machine are added to the System Inventory.

Install 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.

---

**Note**

You do not need to configure the AW DB on both the Publisher and the Subscriber. The configuration is replicated between the Publisher and the Subscriber.

---

**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](page126).

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]
```

For more information, see [set live-data aw-access](page250).

**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]
```

---

**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
```

**Restart Live Data**

After you complete the configuration procedures for the AW and the Unified Intelligence Center data source, restart the Live Data system to enable the changes.

**Procedure**

Access the Live Data CLI and run the following command:

```
util system restart
```
Uninstall Unified CCE Release 11.6(1)

Uninstall Methods

When you uninstall Unified CCE Release 11.6(1), you must choose one of two methods of uninstallation:

- Temporary - leaves the schema unmodified
- Permanent - reverts the database schema to the previous schema version

The option to temporarily or permanently uninstall Unified CCE Release 11.6(1) appears only when you try to perform this task on a machine that is running the following components:

- Logger
- AW only
- HDS
- AW-HDS

Temporary Uninstallation

In a temporary uninstallation, the schema that was updated during the upgrade process does not revert to Unified CCE Release 11.6(1). Use this method of uninstallation when you want to rerun the Unified CCE Release 11.6(1) installer to fix initial installation issues. This method is also useful when you want to upgrade to a future maintenance release.
The Logger, AW, and HDS components check the version table in the ICM database schema for their corresponding schema version. If the versions of the schema and the executable do not match, the system generates an error message and the services are shut down. This error is captured in the component logs.

**Permanent Uninstallation**

In permanent uninstallation, both the application and the database schema change. Uninstalling the upgrade returns the system and the database to previous 11.x version.

A permanent uninstallation is necessary if you wish to revert to previous version of Unified CCE Release 11.x.

**Note**

Configuration data may change when you revert to previous version of Unified CCE Release 11.x:

- Newly added non-voice PQs are converted to voice PQs.
- Agent login names that exceed 32 characters are truncated.

Use the data from the previous version of Unified CCE Release 11.x, configuration database or the virtual machine which you backed up before starting the upgrade process.

If you have used the ICMDBA tool to create an Outbound Option database on Logger Side B, you can manually delete the database after the uninstall by using SQL Server Management Studio (SSMS). If you have enabled Outbound Option two-way replication, you must disable replication from both Logger Side A and Logger Side B before you can delete the database.

**Important**

If there are any database schema rollback errors encountered during permanent uninstall, the database schema may be in a corrupted state. The state prevents CCE Logger / Distributor services to start correctly due to schema mismatch. To recover from the state, the ICMDBA tool can be used to recreate the Logger or HDS database that may have failed.

Configuration data lost due to the schema rollback failure on the logger database, can be recovered by re-importing the configuration database backup that the patch installer would have taken, during 11.6(1) upgrade.

**Note**

Routing Scripts which has dynamic queues configured for skill group node will not be accessible after permanent rollback to previous version of Unified CCE Release 11.x.

**Rollback Caveats**

The section provides following information about permanent Rollback to version 11.0(x):
1. Routing Scripts which have dynamic queues configured for skill group node are not accessible after permanent rollback to previous version of Unified CCE Release 11.x.

2. SSO global and agent/supervisor level configuration, if set, will be removed after rollback to 11.0(x).

3. Agent or Supervisor login names in UPN format gets converted to user account name (netbios name) only. Any login name which exceeds 32 characters gets truncated.

4. If the deployment type has been set to the newly introduced UCCE 2000 Agents Roper deployment type, then the installer would prevent any rollback to the previous version, unless the deployment type is changed to a deployment type like UCCE 4000 Agents, that is supported in the previous release.

5. Unified CCE 11.6(1) has configuration limits enhanced for some of the deployment types. The configuration limits do not get reverted back after performing a rollback to previous version. One would have to reset the previous deployment type again using CCE Admin tool to reset the configuration limit.


6. Newly Added non-voice PQs are converted to voice PQs rollback to 11.0(x).

7. If Outbound Option is enabled with or without high availability on LoggerB side, permanent uninstallation of 11.6(1) is not allowed. Disable outbound option on LoggerB database before performing uninstallation of 11.6(1).

8. Upgraded Java 1.8_0_121 are not removed after uninstallation.

**Revert Tomcat**

For detailed information on the results from each step, see the ../UpgradeTomcatResults/UpgradeTomcat.log file.

**Procedure**

**Step 1**
From the command line, navigate to the directory where you copied the Upgrade Tomcat Utility.

**Step 2**
Enter this command to run the tool: `java -jar UpgradeTomcatTool-<version>.jar -revert`

For example:

```
java -jar UpgradeTomcatTool-11.5.1.jar -revert
```

**Step 3**
When prompted, enter `yes` to continue with the reversion.

**Step 4**
Repeat these steps for all unified CCE component VMs.
Uninstall Unified CCE Release 11.6(1)

This procedure assumes that you are uninstalling the Unified CCE Release 11.6(1) upgrade from a machine that is running the database.

If you have enabled the optional feature Outbound Option High Availability, you must disable it before you can uninstall the upgrade. From Unified CCE Web Setup, choose Component Management > Loggers. Select a logger that is enabled for High Availability, and click Next until the Additional Options page appears. Uncheck the Enable High Availability check box. Perform this action for each logger enabled for Outbound Option High Availability.

**Procedure**

**Step 1** Log in to your system as a user with administrative privileges.

**Step 2** Choose Control Panel > Programs and Features > Cisco ICM Minor Release ICM 11.6(1) > Uninstall. The InstallShield Wizard launches.

**Step 3** Select either permanent or temporary uninstallation.

a) If you choose temporary uninstallation, follow the on-screen instructions to temporarily uninstall the application.

b) If you choose permanent uninstallation and you have enabled Outbound Option High Availability, a message appears informing you that you disable High Availability before you can proceed with the uninstallation. Disable High Availability, and then restart the upgrade uninstallation process.

If you have set UCCE: 2000 Agents Logger deployment, a message appears. The message informs you to change the deployment type before you uninstall the Unified CCE Release 11.6.

**Step 4** On the Database Schema Rollback window, specify if you want to proceed with the uninstallation.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Go to step 5</td>
</tr>
<tr>
<td>No</td>
<td>The uninstallation process cancels</td>
</tr>
</tbody>
</table>

**Step 5** On the confirmation window, click Yes.

**Step 6** (Optional) On the Installation Messages window, click Next.

Post Installation Window specifies if any service is set to manual than a pop-up window displays a notification that some services were automatically changed to manual as part of the uninstallation. Make sure that both A and B sides of your system operate properly after uninstalling Unified CCE Release 11.6(1). Then, set the ICM services that were changed during the uninstallation back to their original setting (Automatic).

**Step 7** At the prompt, restart the machine.

The Unified CCE Release 11.6(1) application is uninstalled from your machine.
Uninstallation of base CCE 11.0(1)

Unified CCE supports the uninstall option from the Programs and Features window in the Windows Control Panel. This option removes the patches, base version files, and the related registry. The specific option also removes Unified CCE component software installed by the ICM-CCE-Installer.

However, it does not remove the following:

- Java Runtime Environment
- Unified CCE databases

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

Uninstalling Unified CCE 11.0(1) removes all traces of the software. You cannot roll back to a previous major version. The option to roll back is only available with maintenance releases.

If you have used the ICMDBA tool to create an Outbound database on Logger Side B, you can manually delete the database after the rollback by using SQL Server Management Studio (SSMS). If you have enabled Outbound Option two-way replication, you must disable replication from both Logger Side A and Logger Side B before you can delete the database.
Testing

- Testing Overview, on page 243
- Testing Tasks, on page 243

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:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that error messages did not display during the upgrade process.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the upgrade logs for error messages.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Ensure that the Unified CVP Operations, Administration, Monitoring and Provisioning (OAMP) Web interface is available for use.</td>
</tr>
</tbody>
</table>
Step 4 Use the diagnostic page at http://<CVPHOST>:8000/cvp/diag to verify the status of the Unified CVP system.

Step 5 Use the Operations Console (System > Control Center, Device Pool tab) to verify that the upgraded Unified CVP Call Servers, Unified CVP VXML Server and Unified CVP Reporting Server show a status of “Up”.

Step 6 Use the Operations Console (Device Management > Unified CVP Call Server, General tab for selected Call Server) to verify that the Device Version reflects the correct upgraded version.

Step 7 Verify that the appropriate voice prompt is heard when the call is made.

Step 8 Ensure that the Unified CVP license is properly installed.

---

**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:
  
  ping or traceroute

**Step 2** Ensure that the following devices are configured and registered correctly: Gatekeeper, trunks, and CTI Route Point.

**Step 3** Ensure that all MGCP end points (FXS, FXO, PRI, T1 CAS and BRI) are properly registered with Unified Communications Manager.

**Step 4** Manually spot check calls as appropriate from the PSTN vis SIP Gateways.
### Verify Upgrade to Cisco IOS-Based Transcoders and Conference Bridges

After upgrading Cisco IOS-based transcoders and conference bridges, verify the following:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Check if the complete configuration before the upgrade still exists.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Check if all DSPs are registered and are functioning normally.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Check if there are no error messages in the buffer log or console.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Check if no dump file is created in the flash memory.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>To verify that the configuration is not lost, type the “show running-config” command.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>To verify that the interfaces are in up state, type the “show ip interface brief” command.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Verify IOS Transcoding is working with G711 codec configure for one device while G729 codec is configured on another device.</td>
</tr>
</tbody>
</table>

### Verify Upgrade to Cisco Unified CCE Router and Logger

After upgrading the Cisco Unified CCE Router and Logger, verify the following:

#### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Verify basic operations such as the following:</td>
</tr>
<tr>
<td></td>
<td>• 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).</td>
</tr>
<tr>
<td></td>
<td>• All components can “ping” public and private IP addresses as applicable.</td>
</tr>
<tr>
<td></td>
<td>• Schema upgrade is successful for all databases and there is no loss of data integrity or data.</td>
</tr>
<tr>
<td></td>
<td>• All component services start correctly without generating errors.</td>
</tr>
<tr>
<td></td>
<td>• Firewalls and other security measures do not block the ability to access Microsoft SQL Server and to run third-party software components, like VNC or PCAnywhere.</td>
</tr>
<tr>
<td></td>
<td>• Ccagent is in service and connected to any Peripheral Gateways located in Side A.</td>
</tr>
<tr>
<td></td>
<td>• Recovery process not required, no activity other than process start-up.</td>
</tr>
<tr>
<td></td>
<td>• Configuration information is passed to the Router by the Logger. Replication process begins when the Historical Database Server comes online.</td>
</tr>
<tr>
<td></td>
<td>• Replication process begins with no errors. (Use the Windows Event Viewer to view Windows Event logs).</td>
</tr>
</tbody>
</table>
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 (for 11.0, icmsetup.txt and ICMInstall.txt, located in the \Temp directory of the disk on which the application was installed and for 11.6 Minor Release YYYYMMDD_HHmmSS_Minor Release ICM11.6(1).log located in the C:\Temp\Minor Release ICM11.6(1) 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.
- Rtsvr, 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:

**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 real time and historical data is sent to the Router and AW database.

**Step 3** Ensure that basic calls and call functionality (such as transfers, conferences, call treatment and queuing) are working properly.

**Step 4** Ensure that the peripheral is running properly on the upgraded gateway by verifying call flows, CTI desktops, Outbound Option, and other applications.

### 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 Cisco Unified Communications Manager

After upgrading Unified Communications Manager, verify the following:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Verify that no error messages have occurred during the upgrade process.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the upgrade log file for any errors.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Start all first node and subsequent node servers.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Verify that there is no replication failure between the first node and subsequent node servers.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Verify that SIP and SCCP IP Phones are registered with Unified Communications Manager.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Ensure that the following devices are configured correctly: gatekeeper, trunks, and CTI route points.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Ensure that the media resources (conference bridges, MTP and transcoders) are configured correctly by checking their status.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Verify if the end users are able to connect to their CTI managers.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Check if the license usage is correct as reported in the License Unit Report.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Check if services on all servers in the cluster are up.</td>
</tr>
</tbody>
</table>
| 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. |
CLI Commands

- Live Data CLI Commands, on page 249
- Transport Layer Security CLI Commands, on page 255

Live Data CLI Commands

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)
- ".!" (exclamation mark)
- ".@" (at sign)
- ".#" (number sign)
- ".$" (dollar)
- ".%" (percent)
- ".^" (caret)
- ".*" (star)
- "._" (underscore)
- ".+" (plus sign)
- ".=" (equal sign)
- ".~" (tilde)
- ".:" (colon)
- "(" and ")" (open and close parentheses)
- "{" and "}" (open and close brackets)
- "[" and "]" (open and close square brackets)
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.

Privilege Levels for Live Data Commands

The Live Data CLI commands support the following privilege levels:

- Ordinary
- Advanced

Each Live Data command has a required privilege level related to the sensitivity of data it exposes or its ability to severely affect the operation of the application. The privilege level for each command is the minimum level required; a user with a higher privilege level also has access to the command.

The Cisco Voice Operating System (VOS) also supports a higher privilege level for the administrative user; this user is configured at installation. When the administrative user creates other users (with the set account name command), the administrative user sets each newly created user’s privilege level. (For more information about the set account command, see the Administration Console User Guide for Cisco Unified Intelligence Center at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.)

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]
```

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 126
Configure Live Data with AW, on page 73

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 126

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, restart the publisher and then the subscriber. Restart the inactive node and then the active node by using the `util system restart` command. (For more information about the command, refer to the Administration Console User Guide for Cisco Unified Intelligence Center at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.)

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 252

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**

```text
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**

```text
unset live-data reporting-interval
```

When you reset the Live Data reporting interval, restart the publisher and then the subscriber. Restart the inactive node and then the active node by using the `utilis system restart` command. (For more information about the command, refer to the *Administration Console User Guide for Cisco Unified Intelligence Center* at [https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html](https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html).)

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 252

---

**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**

```text
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 \texttt{CUIC} as the domain with the user name (for example, \texttt{CUIC\textbackslash administrator}).

This user must have system configuration administrative privileges.

\texttt{cuic-pwd}

Specifies the password to use for authentication with Cisco Unified Intelligence Center.

\texttt{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:

\begin{itemize}
  \item Set the AW DB connection information on the same node where you want to run this command.
  \item Configure Live Data endpoints in the Machine Service table.
\end{itemize}

\textbf{Command Syntax}
\begin{verbatim}
show live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd
\end{verbatim}

\texttt{cuic-addr}

Specifies the Cisco Unified Intelligence Center publisher node's fully qualified domain name (FQDN).

\texttt{cuic-port}

Specifies the Cisco Unified Intelligence Center REST API port. Typically this port is 8444.

\texttt{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 \texttt{CUIC} as the domain with the user name (for example, \texttt{CUIC\textbackslash administrator}).

\texttt{cuic-pwd}

Specifies the password to use for authentication with Cisco Unified Intelligence Center.

\texttt{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:

\begin{itemize}
  \item Set the AW DB connection information on the same node where you want to run this command.
  \item Configure Live Data endpoints in the Machine Service table.
\end{itemize}

\textbf{Command Syntax}
\begin{verbatim}
unset live-data cuic-datasource cuic-addr cuic-port cuic-user cuic-pwd
\end{verbatim}

\texttt{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.

Transport Layer Security CLI Commands

Note
These CLI commands are only for VOS systems. They are not available for VMs running Windows Server 2012 R2.
**TLS Server Minimum Version**

**set tls server min-version**

Use this command to set the current TLS minimum version for inbound connections.

**Command Syntax**

```
set tls server min-version {1.0|1.1|1.2}
```

- **1.0**
  Specifies the TLS server minimum version 1.0 for inbound connections.
- **1.1**
  Specifies the TLS server minimum version 1.1 for inbound connections.
- **1.2**
  Specifies the TLS server minimum version 1.2 for inbound connections.

**show tls server min-version**

Use this command to display the current TLS minimum version for inbound connections.

**Command Syntax**

```
show tls server min-version
```

**TLS Client Minimum Version**

**set tls client min-version**

Use this command to set the current TLS minimum version for outbound connections.

**Command Syntax**

```
set tls client min-version {1.0|1.1|1.2}
```

- **1.0**
  Specifies the TLS client minimum version 1.0 for outbound connections.
- **1.1**
  Specifies the TLS client minimum version 1.1 for outbound connections.
- **1.2**
  Specifies the TLS client minimum version 1.2 for outbound connections.

**show tls server min-version**

Use this command to display the current TLS minimum version for inbound connections.

**Command Syntax**

```
show tls server min-version
```
# Certificates for Live Data Standalone

- Certificates and Secure Communications, on page 257
- Export Self-Signed Live Data Certificates, on page 258
- Import Self-Signed Live Data Certificates, on page 259
- Produce Certificate Internally, on page 260
- Deploy Root Certificate for Internet Explorer, on page 261
- Set Up CA Certificate for Internet Explorer Browser, on page 261
- Set Up CA Certificate for Firefox Browser, on page 262

## 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.

**Note** 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.
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 both Side A and Side B certificates into each side of the Finesses servers.

As is the case when using other self-signed certificates, agents must accept the Live Data certificates in the Finesses desktop when they sign in before they can use the Live Data gadget.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Sign in to Cisco Unified Operating System Administration on the Live Data server (<a href="http://hostname">http://hostname</a> of Live Data server/cmplatform).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the Security menu, select Certificate Management.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Find.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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.)</td>
</tr>
</tbody>
</table>
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 Finesse servers.

Related Topics
Import Self-Signed Live Data Certificates, on page 259

Import Self-Signed Live Data Certificates

To import the certificates into the Finesse servers, use the following procedure.

Procedure

Step 1 Sign in to Cisco Unified Operating System Administration on the Finesse server using the following URL:
http://FQDN of Finesse server:8443/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 258
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.
**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.

To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

**Set Up CA Certificate for Internet Explorer Browser**

After obtaining and uploading the CA certificates, either the certificate must be automatically installed via group policy or all users must accept the certificate.
In environments where users do not log directly into 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.

**Step 13**
Restart the browser for certificate installation to take effect.

**Note**
If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

---

**Set Up CA 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**

**Step 1**
From the Firefox browser menu, select **Options**.

**Step 2**
Click **Advanced**.
Step 3  Click the Certificates tab.
Step 4  Click View Certificates.
Step 5  Click Authorities.
Step 6  Click Import and browse to the ca_name.cer file (in which ca_name is the name of your certificate).
Step 7  Check the Validate Identical Certificates check box.
Step 8  Restart the browser for certificate installation to take effect.
Certificates for Live Data Coresident

- Add Self-Signed Certificates for Live Data, on page 265
- Obtain and Upload CA Certificate for Live Data from a Third Party Vendor, on page 266
- Produce Certificate Internally, on page 266
- Deploy Root Certificate for Internet Explorer, on page 268
- Set Up CA Certificate for Internet Explorer Browser, on page 269
- Set Up CA Certificate for Firefox Browser, on page 269

Add Self-Signed Certificates for Live Data

Both Finesse and Unified Intelligence Center are installed with 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 the Unified Intelligence Center Publisher and Subscriber. You must then import the certificates into Finesse, importing the Publisher certificate to the Finesse Primary node and the Subscriber certificate to the Finesse Secondary node.

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 into Cisco Unified Operating System Administration on Cisco Unified Intelligence Center (https://<hostname of Cisco Unified Intelligence Center 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 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 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.
You must download the certificates that contain the hostnames Cisco Unified Intelligence Center publisher and Cisco Unified Intelligence Center subscriber.

**Step 6** Sign in to Cisco Unified Operating System Administration on the primary Finesse server (https://FQDN of Finesse server:8443/cmplatform).

**Step 7** From the Security menu, select Certificate Management.

**Step 8** Click Upload Certificate.

**Step 9** From the Certificate Name drop-down list, select tomtat-trust.

**Step 10** Click Browse and browse to the location of the .pem files (Cisco Unified Intelligence Center publisher and subscriber certificates).

**Step 11** Click Upload File.

**Step 12** Restart Cisco Finesse Tomcat on the Finesse server.

---

**Obtain and Upload CA Certificate for Live Data from a Third Party Vendor**

You can use a Certification Authority (CA) certificate provided by a third-party vendor to establish an HTTPS connection between the Finesse and Cisco Unified Intelligence Center servers.


**Produce Certificate Internally**

**Set up Microsoft Certificate Server for Windows 2008 R2**

This procedure assumes that your deployment includes a Windows Server 2008 R2 (Standard) Active Directory server. Perform the following steps to add the Active Directory Certificate Services role on the Windows 2008 R2 (Standard) domain controller.

**Procedure**

**Step 1** Click Start, right-click Computer, and select Manage.

**Step 2** In the left pane, click Roles.

**Step 3** In the right pane, click Add Roles.

The Add Roles Wizard opens.

**Step 4** On the Select Server Roles screen, check the Active Directory Certificate Services check box, and then click Next.

**Step 5** On the Introduction to Active Directory Certificate Services screen, click Next.

**Step 6** On the Select Role Services screen, check the Certification Authority check box, and then click Next.
Step 7
On the Specify Setup Type screen, select Enterprise, and then click Next.

Step 8
On the Specify CA Type screen, select Root CA, and then click Next.

Step 9
Click Next on the Set Up Private Key, Configure Cryptography for CA, Configure CA Name, Set Validity Period, and Configure Certificate Database screens to accept the default values.

Step 10
On the Confirm Installations Selections screen, verify the information, and then click Install.

---

**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.

To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1  On the Windows domain controller, navigate to Administrative Tools > Group Policy Management.

Note  Users who have strict Group Policy defined on the Finesse Agent Desktop are required to disable Cross Document Messaging from Group Policy Management to ensure proper functioning of Finesse on Internet Explorer 11.

Step 2  Right-click Default Domain Policy and select Edit.

Step 3  In the Group Policy Management Console, go to Computer Configuration > Policies > Window Settings > Security Settings > Public Key Policies.

Step 4  Right-click Trusted Root Certification Authorities and select Import.

Step 5  Import the `ca_name.cer` file.


Step 7  From the Configuration Model list, select Enabled.

Step 8  Sign in as a user on a computer that is part of the domain and open Internet Explorer.

Step 9  If the user does not have the certificate, run the command `gpupdate.exe /target:computer /force` on the user's computer.
Set Up CA Certificate for Internet Explorer Browser

After obtaining and uploading the CA certificates, either the certificate must be automatically installed via group policy or all users must accept the certificate.

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.

Step 13  Restart the browser for certificate installation to take effect.

*Note*  If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

Set Up CA 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>Description</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>Authorities</strong>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <strong>Import</strong> and browse to the <em>ca_name.cer</em> file (in which <em>ca_name</em> is the name of your certificate).</td>
</tr>
<tr>
<td>Step 7</td>
<td>Check the <strong>Validate Identical Certificates</strong> check box.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Restart the browser for certificate installation to take effect.</td>
</tr>
</tbody>
</table>

The steps provided are for installing a certificate in a Firefox browser.
Migrate from Co-resident Deployment to Standalone Deployment

Upgrade from Co-resident to Standalone Deployments

If your solution exceeds the configuration limits of 2000 Agent Reference Design, use a Reference Design with higher limits and replace the co-resident deployment of CUIC with a standalone deployment of CUIC, Live Data, and IdS. A standalone deployment allows higher capacity and increased reporting end users. You cannot convert the existing co-resident server to a standalone server.

You can export the CUIC reports from the co-resident deployment and import them into the new standalone CUIC.

For a new standalone deployment, you must perform fresh install of the following servers, using the method outlined below:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Set up the System Inventory for Standalone Deployment, on page 272</td>
</tr>
<tr>
<td>3</td>
<td>Install Live Data. See Live Data Standalone Installation, on page 69.</td>
</tr>
</tbody>
</table>
Set up the System Inventory for Standalone Deployment

Procedure

**Step 1**
In Unified CCE Administration, navigate to **System > Deployment**.

**Step 2**
Add the new machine to the System Inventory:

a) Select the co-resident machine to remove. Click **Delete**.

b) Click **New**. The **Add Machine** popup window opens.

c) From the **Type** drop-down menu, select the following machine type:

   Unified Intelligence Center Publisher.

d) In the **Hostname** field, enter the FQDN, hostname, or IP address of the machine.

   The system attempts to convert the value you enter to FQDN.

e) Enter the machine's Administration credentials.

f) Click **Save**.

The machine and its related Subscriber or Secondary machine are added to the System Inventory.

What to do next

If you remove a component from your deployment, delete it from your System Inventory. If you add the component again, or add more components, add those components to the System Inventory.
APPENDIX E

IPv6 Configuration

- Configure NAT64 for IPv6-Enabled Deployment, on page 273
- Set Up IPv6 for VOS-Based Contact Center Applications, on page 275

Configure NAT64 for IPv6-Enabled Deployment

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: https://www.cisco.com/c/en/us/products/collateral/ios-nx-software/enterprise-ipv6-solution/white_paper_c11-676278.html

NAT64 is NOT supported on M train IOS. T train is required.


The following example network diagram and interface configuration demonstrates Stateful NAT64 translation between an IPv6 network and an IPv4 network.

```
interface GigabitEthernet0/0
description ipv4-only interface
```

Note: The following example network diagram and interface configuration demonstrates Stateful NAT64 translation between an IPv6 network and an IPv4 network.

[Network Diagram]

interface GigabitEthernet0/0
description ipv4-only interface

Windows 2012 Domain Controller with DNS
IPv6 Address: 2001:3:94 Default GW: 2001:1
AAAA Record: hostname.domain.com
AAAA Address: 3001:4A4-A5
IPv4 Address: 10.10.10.10 Default GW: 10.10.10.1
IPv6-only Interface
IPv4-only Interface
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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In Windows, navigate to Administrative Tools &gt; DNS. This opens the DNS Manager.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Forward lookup zone, navigate to your deployment's domain name.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click the domain name and select New Host (A or AAAA).</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the New Host dialog box, enter the computer name and IP address of the AW.</td>
</tr>
</tbody>
</table>

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**

Optionally, DNS64 can be used in place of static DNS entries. Use of DNS64 helps facilitate translation between IPv6 and IPv4 networks by synthesizing AAAA resource records from A resource records.


---

### Set Up IPv6 for VOS-Based Contact Center Applications

By default, only IPv4 is enabled for Unified Communications Manager, Cisco 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.

**Procedure**

1. Sign into Cisco Unified Operating System Administration on the Publisher/Primary node:
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`
**INDEX**

| A | configuring (continued)  
|   | Network VRU 103  
|   | CTI Server 52, 53  
|   | Adding 52  
|   | adding a component 52  
|   | completing setup 53  
|   | setting component properties 53  
|   | setting Network Interface Properties 53  
|   | setting properties 52  
| B | data 121, 122, 123  
|   | editing range 123  
|   | file format, importing/exporting 121  
|   | selecting 122  
|   | data sources 127, 128  
|   | adding 128  
|   | Unified CCE 127  
|   | defining 96, 104  
|   | Network VRU label 104  
|   | user variable 96  
|   | dialed number 91  
|   | configuring 91  
| C | expanded call context 95  
|   | defining variable 95  
|   | setting Enabled option 95  
|   | Expanded Call Context (ECC) variables 94  
|   | configuring for CTI Server 94  
| D | import 21, 24, 73, 81  
|   | installing 21, 24, 73, 81  
|   | Microsoft SQL Server 24  
|   | Microsoft Windows Server 21  
|   | VMware tools 73, 81  
|   | ISO files 20  
|   | mount and unmount 20  

**A**

accessing 119

Bulk Configuration tools 119

Active Directory 133

and supervisors 133

configuring 133

adding 112, 128, 133

attributes 112

data sources 128

super users 133

Administration Client installer 54

running installer 54

Administration UI 125

logging in 125

agent 97, 102, 111

assigning to a skill group 111

configuring 97

configuring agent teams 102

agent desk settings 98, 100

configuring 100

in Unified ICM/CCE/CCH 98

Ring No Answer feature 98

applying 123, 124

range of values to a range of fields in a column 124

single value to a range of edit-control fields 123

single value to a range of selection-box fields 123

attributes 112

adding 112

**B**

Bulk Configuration tools 119

accessing 119

**C**

call type 92

configuring 92

CG 53

Private Interfaces 53

Visible Interfaces 53

collation 24

configuring 94, 103

Expanded Call Context (ECC) variables for CTI Server 94
ISO files (continued)
  mounting 20

L
Live Data Primary 70, 77, 230
  Install 70, 77, 230
Live Data Secondary 72, 79, 232
  install 72, 79, 232
login 125, 133, 134
  for supervisors 133
  to the Administration UI 125
  to Unified Intelligence Center Reporting 134

M
Media Routing Domains 87
  configuring for media classes 87
Microsoft SQL Server 24
  install 24
Microsoft Windows Server 21
  install 21
MR PG 49
  setting up 49

N
Network VRU 104, 105
  configuring a script 105
  script 104
Network VRU Bank 89
  configuring 89
Network VRUs 103, 104
  configuring 103
  defining a label 104
  setting default Network VRU and range of correlation numbers 104
Node Manager 53

P
PG 53
  Private Interfaces 53
  precision queues 116, 117
  Consider If 116, 117
  expressions 117
  steps 117
  Wait for 117
Private Interfaces 53

R
records 119, 122
  inserting new 119
  selecting 122
  selecting one field in multiple records (continued) 122
report templates 135
  importing 135
Ring No Answer feature 98
  with Unified CVP 98
route 118
  configuring 118
routin 106
  scripts 106

S
schema upgrade 207
script editor 207
scripts 105, 106
  administrative 106
  Network VRU 105
  routing 106
  troubleshooting 105
selecting 122
  one field in multiple records 122
  records 122
service members 111
  configuring 111
services 89
  configuring 89
setting 95, 104
  default Network VRU and range of correlation numbers 104
  expanded call context Enabled option 95
  expanded call context variable 95
skill group 110
  configuring 110
super users 133
  adding 133

T
tasks 95, 96, 103, 104, 119, 120, 122, 123, 124
  how to access the Bulk Configuration tools 119
  how to apply a range of values to a range of fields in a column 124
  how to apply a single value to a range of edit-control fields 123
  how to apply a single value to a range of selection-box fields 123
  how to configure a Network VRU 103
  how to define a Network VRU label 104
  how to define a user variable 96
  how to define the expanded call context variable 95
  how to import data 120
  how to insert new records 120
  how to select one field in multiple records 122
  how to select records 122
  how to set the default Network VRU and range of correlation numbers 104
  how to set the expanded call context Enabled option 95
timezones 128
  and data sources 128
translation routing 108
  configuring in Unified ICM/CCE/CCH 108
trunk groups 87
  configuring 87

U
Unified CCE data source 127
Unified CVP report templates 135
  importing 135
Unified CVP reporting users 133
  authentication for Unified IC 133
Unified IC reporting users 135
Unified ICM/CCE 87
  trunk groups 87
Unified ICM/CCE/CCH 86, 89, 104, 111
  agent desk settings 98
  Configuration Manager defined 86

Unified ICM/CCE/CCH (continued)
  Network VRU Bank 89
  Network VRU script 104
  service members 111
Unified Intelligence Center 128
  data sources 128
Unified Intelligence Center Reporting 134
  logging in 134
user variables 96
  defining 96

V
virtual machines 18
  create from OVAs 18
Visible Interfaces 53
VMware tools 73, 81
VRU 106
  error checking 106