CONTENTS

PREFACE

Preface ix

Change History ix

About This Guide ix

Audience x

Related Documents x

Communications, Services, and Additional Information xi

Field Alerts and Field Notices xi

Documentation Feedback xi

Conventions xi

PART I

Preparation 13

CHAPTER 1

System Requirements 1

Set up Active Directory 1

Transport Layer Security Version 1.2 Required 1

Installation Tools 2

VMware Hosting and Hardware Support 2

Software Compatibility 2

Software Licenses 2

CHAPTER 2

Prepare Customer Site Servers 5

Prepare Customer Site Servers 5

Prepare Cisco UCS C-Series Customer Site Servers 5

Configure RAID for C240 M4SX 5

Configure RAID for C240 M5SX 6

Install VMware vSphere ESXi 6
Add the Datastores to the Host Server 6
Add the Customer ESXi Host to the vCenter 6
Run the RAID Config Validator Utility 6
NTP and Time Synchronization 7
Global Catalog Requirements 9

CHAPTER 3

Network Design Considerations 11
Network Design Considerations 11
Bandwidth Provisioning and Network QoS Considerations 11

PART II

Installation 13

CHAPTER 4

Packaged CCE 2000 Agents Installation 15
Installation Tasks 15
Create Virtual Machines for Components 16
Create VM for Unified CCE PG 16
Create VM for Unified CCE Rogger 17
Create VM for Unified CCE AW-HDS-DDS 17
Create VMs for the Cisco Unified Customer Voice Portal Servers 18
Install Media Server 19
Create VM for Cisco Unified Communications Manager Publisher 19
Create VM for Cisco Unified Communications Manager Subscriber 19
Create VM for Cisco Finesse Primary 20
Create VM for Cisco Finesse Secondary 20
Create VM for Cisco Unified Intelligence Center Publisher 21
Create VM for Cisco Unified Intelligence Center Subscriber 21
Create VM for Cisco Unified CVP Reporting Server 21
Create VM for Cloud Connect Publisher 22
Create VM for Cloud Connect Subscriber 22

CHAPTER 5

Packaged CCE 4000 Agents Installation 23
Installation Tasks 23
Create Virtual Machines for Components 24
Create VM for Unified CCE PG 24
Chapter 6

Packaged CCE 12000 Agents Installation 31
Installation Tasks 31
Create Virtual Machines for Components 32
Create VM for Unified CCE Logger 32
Create VM for Unified CCE Router 33
Create VM for Unified CCE AW-HDS 33
Create VM for Unified CCE HDS-DDS 33

Part III

Chapter 7

Version Upgrade 35
Upgrade Overview 37
Prerequisites and Important Considerations 37
NTP Configuration Requirements 38
Upgrade Considerations 38
Silent Upgrade 39
Unified CCE Upgrade Overview 40

Chapter 8

Common Ground Upgrade Process 41
Packaged CCE 2000 Agents Deployment 41
Common Ground Upgrade Process 41
Redundant Upgrade Workflow 41
Multistage Upgrade Workflow 49
Hardware Refresh with Common Ground Upgrade 55
Packaged CCE 4000 Agents Deployment 56
Common Ground Upgrade Process 56
Multistage Upgrade Workflow 56
Packaged CCE 12000 Agents Deployment 63
Common Ground Upgrade Process 63
Multistage Upgrade Workflow 63

APPENDIX A

Security Considerations 71
Update the Java Runtime Environment (Optional) 71
Upgrade Tomcat Utility 72
Upgrade Tomcat 72
Revert Tomcat 73

APPENDIX B

Reference 75
Tasks Common to Virtual Machines 75
About Creatings VMs 75
Open Virtualization Files 75
Mount ISO Files 76
Unmount ISO File 76
Create a Virtual Machine from the OVA 76
Configure DNS Server 78
Configure Database Drive 79
Install Antivirus Software 80
Verification of the Downloaded ISO 81
Software Installations for Components 82
Install Microsoft Windows Server 82
Install Microsoft SQL Server 83
Increase Database and Log File Size for TempDB 86
Collation and Locale Settings for Localization 87
Install VMware Tools 87
Create an HDS Database for the External HDS 108
Configure the External HDS 108
Configure Unified Intelligence Center SQL User Account on the External HDS 109
Add a UCCE Instance 110
Set Live Data Secondary Node 110
Set IdS Subscriber Node 110
Install Enterprise Chat and Email 111
Install Cisco Virtualized Voice Browser 112
Install the Language Pack 112
Set Cloud Connect Secondary Node 112
Initial Configuration for Cloud Connect in 4000 and 12000 Agents 113
Common Software Upgrade Procedures 113
Run EDMT 113
Upgrade VMware vSphere ESXi 114
Upgrade Unified CVP Reporting Server 114
Upgrade Cisco Voice Gateway IOS Version 114
Install Cisco JTAPI Client on Unified Communications Manager PG 115
    Install Cisco JTAPI Client on Unified Communications Manager, Release 12.0 and above 115
Upgrade Cisco JTAPI Client on the Unified Communications Manager PG 116
Disable Outbound Options High Availability (If Applicable) 117
Database Performance Enhancement 117
    Performance Enhancement of TempDB 117
    Performance Enhancement of Logger Database 118
    Performance Enhancement of AW-HDS Database 119
Simple Network Management Protocol 120
Preface

- Change History, on page ix
- About This Guide, on page ix
- Audience, on page x
- Related Documents, on page x
- Communications, Services, and Additional Information, on page xi
- Field Alerts and Field Notices, on page xi
- Documentation Feedback, on page xi
- Conventions, on page xi

Change History

<table>
<thead>
<tr>
<th>Change</th>
<th>See</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Added Multistage Upgrade Process for Common Ground Upgrade</td>
<td>Version Upgrade</td>
<td></td>
</tr>
<tr>
<td>Updated Tomcat version</td>
<td>Upgrade Tomcat Utility</td>
<td></td>
</tr>
<tr>
<td>Updated the topics to include certificate information</td>
<td>Upgrade Side A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade Side B</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Postupgrade Tasks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update the Java Runtime Environment (Optional)</td>
<td></td>
</tr>
</tbody>
</table>

About This Guide

This guide explains how to install, configure, and upgrade Cisco Packaged Contact Center Enterprise (Packaged CCE).
Packaged CCE is a solution deployment for delivering Cisco Unified Contact Center Enterprise in a virtualized environment. Packaged CCE requires strict adherence to capacity limits that are detailed in the Solution Design Guide for Cisco Packaged Contact Center Enterprise, available at https://www.cisco.com/en/US/products/ps12586/prod_technical_reference_list.html. It is mandatory to follow all rules and requirements stated in the Design Guide.

This document does not discuss the Packaged CCE Lab Only deployment. For information about that deployment, see the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

### Audience

This guide is prepared for partners and service providers who will be implementing Packaged CCE, who are familiar with Cisco contact center applications, and who are experienced regarding the deployment and management of virtual machines using VMware technology.

### Related Documents

<table>
<thead>
<tr>
<th>Subject</th>
<th>Link</th>
</tr>
</thead>
</table>
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Alerts and Field Notices

Note that Cisco products may be modified or key processes may be determined important. These are announced through use of the Cisco Field Alert and Cisco Field Notice mechanisms. You can register to receive Field Alerts and Field Notices through the Product Alert Tool on Cisco.com. This tool enables you to create a profile to receive announcements by selecting all products of interest. Log into www.cisco.com; 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 font</strong></td>
<td>Boldface font is used to indicate commands, such as user entries, keys, buttons, folder names, and submenu names.</td>
</tr>
<tr>
<td></td>
<td>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><em>italic font</em></td>
<td>Italic font is used to indicate the following:</td>
</tr>
<tr>
<td></td>
<td>• To introduce a new term. Example: A <em>skill group</em> 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 (<em>condition, true-value, false-value</em>)</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 font</strong></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: &lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</td>
</tr>
<tr>
<td><code>&lt; &gt;</code></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>
PART I

Preparation

• System Requirements, on page 1
• Prepare Customer Site Servers, on page 5
• Network Design Considerations, on page 11
CHAPTER 1

System Requirements


- Set up Active Directory, on page 1
- Transport Layer Security Version 1.2 Required, on page 1
- Installation Tools, on page 2
- VMware Hosting and Hardware Support, on page 2
- Software Compatibility, on page 2
- Software Licenses, on page 2

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.

Transport Layer Security Version 1.2 Required

Contact center enterprise solutions require the use of TLS 1.2 only connections in this release. Our services accept incoming TLS connections only over TLS 1.2. All outgoing TLS connection use only TLS 1.2. All clients that connect to either our web interfaces or databases must support TLS 1.2.

The older versions of the TLS/SSL are disabled by installer.

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 software of Windows Server.

  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.

  The SQL Server installation disables the Windows Computer Browsers service. The ICMDBA requires this service. If you need to run ICMDBA on this server, enable the Computer Browser service.

- **Domain Manager**—Used to provision Active Directory.

- **Web Setup**—Used to set up the Call Routers, Loggers, Network Gateways, Network Interface Controllers, and Administration & Data Servers.

- **Peripheral Gateway Setup**—Used to set up MR PIMs and CG.

VMware Hosting and Hardware Support

See the [Virtualization for Cisco Packaged CCE](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html) for the supported specification based hardware, Cisco UCS C-Series servers for Packaged CCE fresh installs and upgrades, and supported VMware vSphere ESXi versions.

Software Compatibility


- Endpoints for agents and callers
- Cisco gateway hardware and software
- Third-party software

Software Licenses

The following table lists the Cisco components that comprise a Packaged CCE solution:
## Components

<table>
<thead>
<tr>
<th>Components</th>
<th>License requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Packaged Contact Center Enterprise</td>
<td>One server license for each of the voice applications. One agent license for each concurrent user with different feature tiers.</td>
</tr>
<tr>
<td>Cisco Unified Communications Manager</td>
<td>One license for each Cisco Unified Communications Manager node, plus device licenses for connected devices.</td>
</tr>
<tr>
<td>Cisco Finesse</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.</td>
</tr>
</tbody>
</table>

### Note


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

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

Perform all the procedures in this section on the Side A and the Side B servers.

For more information regarding Hyperflex, see the install and upgrade guides available at:
products-installation-guides-list.html.

Prepare Cisco UCS C-Series Customer Site Servers

Configure RAID for C240 M4SX

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

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
- Write Policy: Write Back with BBU
- Read Policy: Read Ahead Always

For more information regarding RAID configuration for C240 M4SX in Configure RAID with GUI (UCS C-Series M4 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/CHCS_BK_C7C7ED05_00_cisco-collaboration-on-virtual-servers_chapter_01.html#CUCM_TK_C2DC4F2D_00.
Configure RAID for C240 M5SX

The disk array configuration for the UCS C240 M5SX is already set up to match the requirements. 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 or 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/CHCS_BK_C7C7ED05_00_cisco-collaboration-on-virtual-servers_chapter_01.html

Install VMware vSphere ESXi

Packaged CCE uses standard VMware vSphere ESXi installation procedures. For installation procedures to install the supported version of vSphere ESXi that you are installing, see the VMware documentation at https://www.vmware.com/support/pubs/.

For Packaged CCE, you must install the ESXi on the first drive as the default boot drive for the server.

Add the Datastores to the Host Server

After installing vSphere ESXi, add the remaining datastores. Refer to the vSphere Storage Guide for the vSphere ESXi version in your deployment, available at https://www.vmware.com/support/pubs/.

Required datastores are dictated by the hardware platform used. Cisco UCS C-Series servers require a fixed and validated configuration.

Add the Customer ESXi Host to the vCenter

Refer to the vCenter Server and Host Management documentation at https://www.vmware.com/support/pubs/

Customers without vCenter can install on management desktops to administer the Packaged CCE servers.

Run the RAID Config Validator Utility

After you set up RAID configuration and add the datastores, run the RAID Config Validator utility to ensure that your datastore configuration is correct.
Before you begin

To run the utility, Java 7 (any update) must be installed. Java 8 and later releases are not supported.

---

Important

Do not use this utility to validate the RAID configurations made for Cisco UCS C240 M5.

---

Procedure

Step 1

Step 2
Open the Windows command prompt and change to the directory where you downloaded the file.

Step 3
Enter this command to run the tool: `java -jar PackagedCCEraidConfigValidator-<version>.jar <IP Address of the Side A ESXi host> <username> <password>`

For example:

```
C:\Users\Administrator\Desktop>java -jar PackagedCCEraidConfigValidator-11.0.jar xx.xx.xxx.xxx userName password
```

Messages appear on the monitor to show that the validation is starting. You then see an indication of a valid or invalid configuration.

Step 4
If your configuration is valid, repeat step 2. Enter the IP address of the Side B server instead of the Side A server.

What to do next

If the utility reports an invalid configuration, you must recreate the RAID configuration. To do this, reset the RAID configuration, re-install ESXi, and then re-run the RAID Config Validator utility to re-validate the configuration.

RAID configuration errors include:

- Non-supported server found or used.
- Incorrect number of datastores found.
- Incorrect sizes set for the datastores.

---

NTP and Time Synchronization

Packaged CCE requires that all parts of the solution have the same time. While time drift occurs naturally, it is critical to configure NTP to keep solution components synchronized.

To prevent time drifts on Live Data reports, the NTP settings on the Roggler VMs, the PG VMs, the AW VMs, and on the Cisco Unified Intelligence Center Publisher and Subscriber VMs must be synchronized.
Microsoft periodically releases cumulative time zone updates. These updates include worldwide changes to time zone names, bias (the amount of time in minutes that a time zone is offset from Coordinated Universal Time (UTC)), and observance of daylight saving time. These patches update the information in the Windows registry. When these updates are available, apply them to all virtual machines in the deployment that are running a Microsoft Windows operating system.

Important

Windows Active Directory Domain

The Windows Active Directory Primary Domain Controller (PDC) emulator master for the forest in which the Packaged CCE domain resides (whether same, parent, or peer) must be properly configured to use an external time source. This external time source should be a trusted and reliable NTP provider, and if already configured for the customer's forest, must be used (and useable) as same source for all other applications as detailed in this section for the Packaged CCE solution.

See the following references for properly configuring Windows Active Directory Domain for NTP external time source:

- How to configure an authoritative time server in Windows Server.

Note

- Do not use the "Fix it for me" function in this article.

- AD DS: The PDC emulator master in this forest should be configured to correctly synchronize time from a valid time source.

Microsoft Windows Server Domains do not automatically recover or fail over the authoritative internal time source for the domain when the PDC emulator master server is lost, due to hardware failure or otherwise. This article, Time Service Configuration on the DC with PDC Emulator FSMO Role, helps describe how you must additionally configure the new target server to be the authoritative internal time source for the domain. It also covers manual intervention to recover and seize or reassign the PDC Flexible Single-Master Operations (FSMO) role to another domain controller.

Windows Components in the Domain

Windows hosts in the domain are automatically configured to synch their time with a PDC emulator, whether by the PDC emulator master with authoritative internal time source or chained from same in the domain forest hierarchy.

Windows Components Not in the Domain

Use the following steps to set NTP time source for a Windows Server that is not joined to a domain:

1. Log in as a user with administrative privileges.
2. In the Command Prompt window, type the following line and press ENTER: `w32tm /config /manualpeerlist:PEERS /syncfromflags:MANUAL`

Note

Replace peers with a comma-separated list of NTP servers.
3. Restart the w32time service: `net stop w32time && net start w32time`.

4. Synch w32time service with peers: `w32tm /resync`.

5. Use the following Service Control command to ensure proper start of the w32time service on any reboot of the server: `sc triggerinfo w32time start/networkon stop/networkoff`.

**Cisco Integrated Service Routers**

Cisco IOS Voice Gateways must be configured to use the same NTP source for the solution in order to provide accurate time for logging and debugging. See [Basic System Management Configuration Guide, Cisco IOS Release 15M&T: Setting Time and Calendar Services](https://www.cisco.com).

**VOS Components**

Components such as Unified Intelligence Center, Finesse, Customer Collaboration Platform, and Unified Communications Manager must point to the same NTP servers as the domain authoritative internal time source.

**CLI commands for NTP Servers**

While NTP servers are typically specified at install time, here a few commands you can use from the platform cli of the above listed components, to list, add and remove ntp servers. From the platform CLI:

- To list existing ntp servers: `utils ntp servers list`
- To add an additional ntp server: `utils ntp server add <host or ip address to add>`
- To delete an existing ntp server: `utils ntp server delete (row number of the item to delete)`. Press Enter.

**ESXi Hosts**

All Packaged CCE ESXi hosts (including those for optional components), must point to the same NTP server(s) used by the Windows domain PDC emulator master as their external time source.

For details on configuring NTP on ESXi hosts, see the VMware documentation at [https://www.vmware.com/support/pubs/](https://www.vmware.com/support/pubs/).

**Global Catalog Requirements**

Packaged CCE uses the Global Catalog for Active Directory Lookup. All domains in the AD Forest in which the Packaged CCE Hosts reside must publish the Global Catalog for that domain. This includes all domains with which your solution interacts, for example, Authentication, user lookup, and group lookup.

In a multi-domain forest, a Global Catalog is required at each AD site. Global Catalog is a central repository of domain information in an AD forest. A significant performance degradations and failure occur without local or Global Catalog. It is important for every AD query to search each domain in the forest. The multi-site deployments are required to query across WAN links.

---

**Note**

This does not imply cross-forest operation. Cross-forest operation is not supported.
Network Design Considerations

• Network Design Considerations, on page 11
• Bandwidth Provisioning and Network QoS Considerations, on page 11

Network Design Considerations


Bandwidth Provisioning and Network QoS Considerations


Bandwidth Provisioning and Network QoS Considerations
PART II

Installation

- Packaged CCE 2000 Agents Installation, on page 15
- Packaged CCE 4000 Agents Installation, on page 23
- Packaged CCE 12000 Agents Installation, on page 31
Packaged CCE 2000 Agents Installation

Installation Tasks

This section provides tasks to create and set up virtual machines (VM) of various components that are required for the Packaged CCE 2000 Agents installation. For information about creating VMs on the appropriate data centers for specific components, see Unified CCE Reference Designs section in the Solution Design Guide for Cisco Unified Contact Center Enterprise guide, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Note

If your Reference Design layout is on the Cisco Hyperflex HX220c M5SX servers, auto-discovery (to identify and validate the components on ESXi servers) is based only on the first node of the Hyperflex cluster.

Note

If your Reference Design layout is on the Cisco UCS C240 M5SX servers, make sure that the following core components are added on-box without changing the default annotations:

- Unified CCE Rogue
- Unified CCE AW/HDS/DDS
- Unified CCE PG
- Unified CVP Server
- Unified Intelligence Center Publisher(with coresident LiveData and IDS)
- Finesse

The following terms are reserved for core component annotations: Cisco, Finesse, CUIC, and CVP. Do not use these reserved terms in the annotations of any of the non-core component VMs.

The table outlines the Packaged CCE 2000 Agents installation tasks.
Create Virtual Machines for Components

Create VM for Unified CCE PG

Follow this sequence of tasks to create a virtual machine for the Unified CCE PG.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>Medium PG</strong> from the drop-down list.</td>
</tr>
</tbody>
</table>

Create VM for Unified CCE Rogger

Follow this sequence of tasks to create a virtual machine for the Unified CCE Rogger.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>Rogger</strong> from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapters, on page 89</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Set Persistent Static Routes, on page 90</td>
</tr>
<tr>
<td>8</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>9</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
</tbody>
</table>

Create VM for Unified CCE AW-HDS-DDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE AW-HDS-DDS.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-UCCE.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>AW-HDS-DDS</strong> from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapters, on page 89</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Configure Database Drive, on page 79</td>
</tr>
<tr>
<td>8</td>
<td>Set Persistent Static Routes, on page 90</td>
</tr>
<tr>
<td>9</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>10</td>
<td>Install Microsoft SQL Server, on page 83</td>
</tr>
<tr>
<td>11</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
</tbody>
</table>
Create VMs for the Cisco Unified Customer Voice Portal Servers

Follow this sequence of tasks to create the virtual machines for the Unified CVP Servers. Each Unified CVP Server combines the Unified CVP Call Server, Media Server, and VXML Server functionality.

### Create VMs for the Cisco Unified Customer Voice Portal Servers

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
</table>
| 1        | Using Packaged-CCE-CVP.ova, Create a Virtual Machine from the OVA, on page 76. From the drop-down list:  
  • Select **Cisco Unified CVP Call Server-VXML Server** from the drop-down list when you create the Unified CVP Server VM. |
| 2        | Install Microsoft Windows Server, on page 82  
  NTP configuration is required if this machine is not in the same domain as the Unified CCE Riggers, AWs, and PGs. See NTP and Time Synchronization, on page 7. |
| 3        | Install VMware Tools, on page 87 |
| 4        | Configure Network Adapters for Cisco Unified CVP, on page 94 |
| 5        | Add Machine to Domain, on page 88 |
| 6        | Install Antivirus Software, on page 80 |
| 7        | Run Windows Updates, on page 91 |
| 8        | Install Cisco Unified CVP Server, on page 95 |
Install Media Server

If the Media Server is external, install the following on the Media Server:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Install FTP Server, on page 97</td>
</tr>
</tbody>
</table>

Create VM for Cisco Unified Communications Manager Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Communications Manager Publisher.

- For the UCS C240 M4 Server, the Unified Communications Manager (CUCM) 12.5 installation must be off-box.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-CUCM.ova. Create a Virtual Machine from the OVA, on page 76. Select CUCM 7500 user node from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Unified Communications Manager Publisher.</td>
</tr>
<tr>
<td></td>
<td>See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>5</td>
<td>Configure the Cluster for Cisco Unified Communications Manager, on page 102</td>
</tr>
<tr>
<td>6</td>
<td>Create a Unified Communications Manager AXL User Account, on page 102</td>
</tr>
<tr>
<td>7</td>
<td>Generate and install the Unified Communications Manager License, on page 101.</td>
</tr>
<tr>
<td>8</td>
<td>Activate Services, on page 106</td>
</tr>
</tbody>
</table>

Create VM for Cisco Unified Communications Manager Subscriber

Follow this sequence of tasks to create the virtual machine for the Cisco Unified Communications Manager Subscriber.
<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-CUCM.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>CUCM 7500 user node</strong> from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Unified Communications Manager Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>5</td>
<td>Generate and install the Unified Communications Manager License, on page 101.</td>
</tr>
<tr>
<td>6</td>
<td>Activate Services, on page 106</td>
</tr>
</tbody>
</table>

### Create VM for Cisco Finesse Primary

Follow this sequence of steps to create a virtual machine for the Cisco Finesse Primary node.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using the Packaged-CCE-Finesse.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>2000 HTTPS Agent</strong> from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Finesse Primary node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>5</td>
<td>Configure the Cluster for Cisco Finesse, on page 103</td>
</tr>
</tbody>
</table>

### Create VM for Cisco Finesse Secondary

Follow this sequence of tasks to create the virtual machine for the Cisco Finesse Secondary node.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-Finesse.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>2000 HTTPS Agent</strong> from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Finesse Secondary node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
</tbody>
</table>
### Create VM for Cisco Unified Intelligence Center Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Publisher. Live Data and the Cisco Identity Service are also installed on the same VM.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-CUIC.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>Co-Resident</strong> from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Unified Intelligence Center Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>5</td>
<td>Configure the Cluster for Cisco Unified Intelligence Center, on page 101</td>
</tr>
</tbody>
</table>

### Create VM for Cisco Unified Intelligence Center Subscriber

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Subscriber. Live Data and the Cisco Identity Service are also installed on this VM.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-CUIC.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>Co-Resident</strong> from the drop-down list.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Unified Intelligence Center Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
</tbody>
</table>

### Create VM for Cisco Unified CVP Reporting Server

Follow this sequence of tasks to create a virtual machine for the Unified CVP Reporting Server. The Unified CVP Reporting Server is an optional component.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-CVP.ova, Create a Virtual Machine from the OVA, on page 76. Select <strong>Cisco Unified CVP Reporting Server</strong> from the drop-down list.</td>
</tr>
</tbody>
</table>
| 2        | Install Microsoft Windows Server, on page 82  
NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 7. |
### Create VM for Cloud Connect Publisher

Follow this sequence of tasks to create the virtual machine for the Cloud Connect Publisher.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-cloudconnect.ova, Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Install the Cloud Connect Publisher. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99.</td>
</tr>
</tbody>
</table>

### Create VM for Cloud Connect Subscriber

Follow this sequence of tasks to create the virtual machine for the Cloud Connect Subscriber.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Using Packaged-CCE-cloudconnect.ova, Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cloud Connect Subscriber. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
<tr>
<td>4</td>
<td>Initial Configuration for Cloud Connect in 4000 and 12000 Agents</td>
</tr>
</tbody>
</table>
Packaged CCE 4000 Agents Installation

Installation Tasks

This section provides the sequence to create and set up virtual machines of various components that are required for the Packaged CCE 4000 Agents fresh installation. For information about creating VMs on the appropriate data centers for specific components, see Unified CCE Reference Designs section in the Solution Design Guide for Cisco Unified Contact Center Enterprise, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

The table outlines the Packaged CCE 4000 Agents fresh installation tasks.

Table 2: Packaged CCE 4000 Agents Installation

<table>
<thead>
<tr>
<th>Component Installation Tasks</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Create VM for Unified CCE PG, on page 24</td>
<td></td>
</tr>
<tr>
<td>2 Create VM for Unified CCE Loggger, on page 24</td>
<td></td>
</tr>
<tr>
<td>3 Create VM for Unified CCE AW-HDS-DDS, on page 25</td>
<td></td>
</tr>
<tr>
<td>4 Create VMs for the Cisco Unified Customer Voice Portal Servers, on page 25</td>
<td></td>
</tr>
<tr>
<td>5 Create VM for Cisco Unified Communications Manager Publisher, on page 26</td>
<td></td>
</tr>
<tr>
<td>6 Create VM for Cisco Unified Communications Manager Subscriber, on page 27</td>
<td></td>
</tr>
<tr>
<td>7 Create VMs for Cisco Finesse Primary Nodes, on page 27</td>
<td></td>
</tr>
<tr>
<td>8 Create VMs for Cisco Finesse Secondary Nodes, on page 28</td>
<td></td>
</tr>
<tr>
<td>9 Create VM for Cisco Unified Intelligence Center Publisher, on page 28</td>
<td></td>
</tr>
<tr>
<td>10 Create VM for Cisco Unified Intelligence Center Subscriber, on page 28</td>
<td></td>
</tr>
<tr>
<td>11 Create VM for Live Data Primary Node, on page 29</td>
<td></td>
</tr>
<tr>
<td>12 Create VM for Live Data Secondary Node, on page 29</td>
<td></td>
</tr>
</tbody>
</table>
Create Virtual Machines for Components

Create VM for Unified CCE PG

Follow this sequence of tasks to create a virtual machine for the Unified CCE PG.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapters , on page 89</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Set Persistent Static Routes, on page 90</td>
</tr>
<tr>
<td>8</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>9</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
</tbody>
</table>

Create VM for Unified CCE Ronger

Follow this sequence of tasks to create a virtual machine for the Unified CCE Ronger.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
</tbody>
</table>
Create VM for Unified CCE AW-HDS-DDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE AW-HDS-DDS.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82.</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87.</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS, on page 90</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Configure Database Drive, on page 79</td>
</tr>
<tr>
<td>8</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>9</td>
<td>Install Microsoft SQL Server, on page 83</td>
</tr>
<tr>
<td>10</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
<tr>
<td>11</td>
<td>Configure Permissions in the Local Machine, on page 92</td>
</tr>
</tbody>
</table>

Create VMs for the Cisco Unified Customer Voice Portal Servers

Follow this sequence of tasks to create the virtual machines for the Unified CVP Servers. Each Unified CVP Server combines the Unified CVP Call Server, Media Server, and VXML Server functionality.
Create VM for Cisco Unified CVP Reporting Server

Follow this sequence of tasks to create a virtual machine for the Unified CVP Reporting Server.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
</tbody>
</table>
| 2        | Install Microsoft Windows Server, on page 82  
NTP configuration is required if this machine is not in the same domain as the Unified CCE Roggers, AWs, and PGs. See NTP and Time Synchronization, on page 7. |
| 3        | Install VMware Tools, on page 87 |
| 4        | Configure Network Adapters for Cisco Unified CVP, on page 94 |
| 5        | Add Machine to Domain, on page 88 |
| 6        | Install Antivirus Software, on page 80 |
| 7        | Run Windows Updates, on page 91 |
| 8        | Install Cisco Unified CVP Server, on page 95 |
| 9        | Install FTP Server, on page 97 |

Create VM for Cisco Unified Communications Manager Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Communications Manager Publisher.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>Sequence</td>
<td>Task</td>
</tr>
<tr>
<td>----------</td>
<td>------</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
</tbody>
</table>
| 3        | Install the Unified Communications Manager Publisher.  
See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99. |
| 4        | Install VMware Tools, on page 87 |
| 5        | Configure the Cluster for Cisco Unified Communications Manager, on page 102 |
| 6        | Create a Unified Communications Manager AXL User Account, on page 102 |
| 7        | Generate and install the Unified Communications Manager License, on page 101. |
| 8        | Activate Services, on page 106 |

### Create VM for Cisco Unified Communications Manager Subscriber

Follow this sequence of tasks to create the virtual machine for the Cisco Unified Communications Manager Subscriber.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
</tbody>
</table>
| 3        | Install the Unified Communications Manager Subscriber.  
See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104. |
| 4        | Install VMware Tools, on page 87 |
| 5        | Generate and install the Unified Communications Manager License, on page 101. |
| 6        | Activate Services, on page 106 |

### Create VMs for Cisco Finesse Primary Nodes

Follow this sequence of steps to create a virtual machine for each of the Cisco Finesse Primary nodes.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
</tbody>
</table>
| 3        | Install the Cisco Finesse Primary node.  
See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99. |
| 4        | Install VMware Tools, on page 87 |
Create VMs for Cisco Finesse Secondary Nodes

Follow this sequence of tasks to create the virtual machine for each of the Cisco Finesse Secondary nodes.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Finesse Secondary node.</td>
</tr>
<tr>
<td></td>
<td>See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
</tbody>
</table>

Create VM for Cisco Unified Intelligence Center Publisher

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Publisher.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Unified Intelligence Center Publisher.</td>
</tr>
<tr>
<td></td>
<td>See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>5</td>
<td>Configure the Cluster for Cisco Unified Intelligence Center, on page 101</td>
</tr>
</tbody>
</table>

Create VM for Cisco Unified Intelligence Center Subscriber

Follow this sequence of tasks to create the virtual machine for the Unified Intelligence Center Subscriber nodes.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Unified Intelligence Center Subscriber.</td>
</tr>
<tr>
<td></td>
<td>See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
</tbody>
</table>
Create VM for Live Data Primary Node

Follow this sequence of steps to create a virtual machine for the Cisco Live Data Primary node.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76. Select <strong>Small Live Data Server</strong> from the drop-down list for 4000 Agents deployment. Select <strong>Larger Live Data Server</strong> from the drop-down list for 12000 Agents deployment.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Live Data Primary node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99.</td>
</tr>
<tr>
<td>4</td>
<td>Install VMware Tools, on page 87</td>
</tr>
</tbody>
</table>

Create VM for Live Data Secondary Node

Follow this sequence of steps to create a virtual machine for the Cisco Live Data Secondary node.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76. Select <strong>Small Live Data Server</strong> from the drop-down list for 4000 Agents deployment. Select <strong>Larger Live Data Server</strong> from the drop-down list for 12000 Agents deployment.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Live Data Secondary node. See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
<tr>
<td>4</td>
<td>Set Live Data Secondary Node, on page 110</td>
</tr>
<tr>
<td>5</td>
<td>Install VMware Tools, on page 87</td>
</tr>
</tbody>
</table>

Create VM for Cisco Identity Service Publisher

Follow this sequence of steps to create a virtual machine for the Cisco Identity Service Publisher node.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Identity Service Publisher node. See Install Publishers/Primary Nodes of VOS-Based Contact Center Applications, on page 99.</td>
</tr>
</tbody>
</table>
Create VM for Cisco Identity Service Subscriber

Follow this sequence of steps to create a virtual machine for the Cisco Identity Service Subscriber node.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Configure DNS Server, on page 78</td>
</tr>
<tr>
<td>3</td>
<td>Install the Cisco Identity Service Subscriber node.</td>
</tr>
<tr>
<td></td>
<td>See Install Subscribers/Secondary Nodes of VOS-Based Contact Center Applications, on page 104.</td>
</tr>
<tr>
<td>4</td>
<td>Set IdS Subscriber Node, on page 110</td>
</tr>
<tr>
<td>5</td>
<td>Install VMware Tools, on page 87</td>
</tr>
</tbody>
</table>
Packaged CCE 12000 Agents Installation

Installation Tasks

This section provides the sequence to create and set up virtual machines of various components that are required for the Packaged CCE 12000 Agents fresh installation. For information about creating VMs on the appropriate data centers for specific components, see Unified CCE Reference Designs section in the Solution Design Guide for Cisco Unified Contact Center Enterprise, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

The table outlines the Packaged CCE 12000 Agents fresh installation tasks.

<table>
<thead>
<tr>
<th>Component Installation Tasks</th>
<th>p.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Create VM for Unified CCE PG</td>
<td>24</td>
</tr>
<tr>
<td>2 Create VM for Unified CCE Logger</td>
<td>32</td>
</tr>
<tr>
<td>3 Create VM for Unified CCE Router</td>
<td>33</td>
</tr>
<tr>
<td>4 Create VM for Unified CCE AW-HDS</td>
<td>33</td>
</tr>
<tr>
<td>5 Create VM for Unified CCE HDS-DDS</td>
<td>33</td>
</tr>
<tr>
<td>6 Create VMs for the Cisco Unified Customer Voice Portal Servers</td>
<td>25</td>
</tr>
<tr>
<td>7 Create VM for Cisco Unified Communications Manager Publisher</td>
<td>26</td>
</tr>
<tr>
<td>8 Create VM for Cisco Unified Communications Manager Subscriber</td>
<td>27</td>
</tr>
<tr>
<td>9 Create VMs for Cisco Finesse Primary Nodes</td>
<td>27</td>
</tr>
<tr>
<td>10 Create VMs for Cisco Finesse Secondary Nodes</td>
<td>28</td>
</tr>
<tr>
<td>11 Create VM for Cisco Unified Intelligence Center Publisher</td>
<td>28</td>
</tr>
<tr>
<td>12 Create VM for Cisco Unified Intelligence Center Subscriber</td>
<td>28</td>
</tr>
</tbody>
</table>
Create Virtual Machines for Components

**Component Installation Tasks**

<table>
<thead>
<tr>
<th>Task Sequence</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Create VM for Live Data Primary Node, on page 29</td>
</tr>
<tr>
<td>14</td>
<td>Create VM for Live Data Secondary Node, on page 29</td>
</tr>
<tr>
<td>15</td>
<td>Create VM for Cisco Identity Service Publisher, on page 29</td>
</tr>
<tr>
<td>16</td>
<td>Create VM for Cisco Identity Service Subscriber, on page 30</td>
</tr>
<tr>
<td>17</td>
<td>Install Cisco Virtualized Voice Browser, on page 112</td>
</tr>
<tr>
<td>18</td>
<td>(Optional) Create VM for Cisco Unified CVP Reporting Server, on page 26</td>
</tr>
<tr>
<td>19</td>
<td>(Optional) Install Media Server, on page 19</td>
</tr>
<tr>
<td>20</td>
<td>(Optional) Install Enterprise Chat and Email, on page 111</td>
</tr>
<tr>
<td>21</td>
<td>(Optional) Install the External HDS, on page 107</td>
</tr>
</tbody>
</table>


Create Virtual Machines for Components

**Create VM for Unified CCE Logger**

Follow this sequence of tasks to create a virtual machine for the Unified CCE Logger.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapters, on page 89</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Configure Database Drive, on page 79</td>
</tr>
<tr>
<td>8</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>9</td>
<td>Install Microsoft SQL Server, on page 83</td>
</tr>
<tr>
<td>10</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
</tbody>
</table>
Create VM for Unified CCE Router

Follow this sequence of tasks to create a virtual machine for the Unified CCE Router.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapters, on page 89</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>8</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
</tbody>
</table>

Create VM for Unified CCE AW-HDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE AW-HDS.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS , on page 90</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Configure Database Drive, on page 79</td>
</tr>
<tr>
<td>8</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>9</td>
<td>Install Microsoft SQL Server, on page 83</td>
</tr>
<tr>
<td>10</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
<tr>
<td>11</td>
<td>Configure Permissions in the Local Machine, on page 92</td>
</tr>
</tbody>
</table>

Create VM for Unified CCE HDS-DDS

Follow this sequence of tasks to create a virtual machine for the Unified CCE HDS-DDS.
<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a Virtual Machine from the OVA, on page 76.</td>
</tr>
<tr>
<td>2</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>3</td>
<td>Install VMware Tools, on page 87</td>
</tr>
<tr>
<td>4</td>
<td>Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS, on page 90</td>
</tr>
<tr>
<td>5</td>
<td>Add Machine to Domain, on page 88</td>
</tr>
<tr>
<td>6</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>7</td>
<td>Configure Database Drive, on page 79</td>
</tr>
<tr>
<td>8</td>
<td>Run Windows Updates, on page 91</td>
</tr>
<tr>
<td>9</td>
<td>Install Microsoft SQL Server, on page 83</td>
</tr>
<tr>
<td>10</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
<tr>
<td>11</td>
<td>Configure Permissions in the Local Machine, on page 92</td>
</tr>
</tbody>
</table>
PART III

Version Upgrade

• Upgrade Overview, on page 37
• Common Ground Upgrade Process, on page 41
Upgrade Overview

- Prerequisites and Important Considerations, on page 37
- Upgrade Considerations, on page 38
- Silent Upgrade, on page 39
- Unified CCE Upgrade Overview, on page 40

Prerequisites and Important Considerations

- After you begin the migration and upgrade process, you cannot back out of it. If you want to go back to the previous release, you must restore your VMs from your backup.

- You can upgrade to Cisco Packaged CCE 2000, 4000, and 12000 Agent deployments, Release 12.5(1) from Release 12.0(x) directly.

- Before you upgrade the Cisco VOS based servers such as the Live Data server, check the Check and upgrade VMware Tools before each power on box in the VM's Options > Edit Settings.

  For more information on VMware Tools upgrade, see the VMware documentation.

- Before upgrading, close all the open Microsoft Windows Event Viewer instances. This will prevent an installation failure with an error that the following DLLs are locked:
  - icrcat.dll
  - icrmmsgs.dll
  - snmpeventcats.dll
  - snmpeventmsgs.dll

  If the failure occurs, close the Event Viewer and retry the installation. If the failure persists, restart the Microsoft Windows Event Log service.

- This release contains an updated database schema. During the upgrade process, perform a schema upgrade using the Enhanced Database Migration Tool (EDMT).

  For the upgrade utilities, see https://software.cisco.com/download/type.html?mdfid=268439622

- Make sure that you have backups of all components in both Side A and Side B before you begin your upgrade. You can take a snapshot of the virtual machines on which you are performing an upgrade.
• After you configure the servers, you can move the VMs to the servers and complete the common ground upgrade process.

• Optionally, you can stage the Unified CCE Rigger off box before you begin the migration and upgrade to lessen your downtime.

• If you already have a Customer Collaboration Platform added in the remote site, it is recommended to delete the Customer Collaboration Platform from the remote site and add it as an External Machine in the Main site. For more information on how to delete and add an external machine, see the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

• Make sure that you are running the minimum supported version of ESXi. For information about supported ESXi versions, see the Virtualization for Cisco Packaged CCE at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html.

NTP Configuration Requirements

Packaged CCE relies on time synchronization. Properly configuring NTP is critical for reliability of reporting data and cross-component communication. It's important to implement the requirements outlined in NTP and Time Synchronization, on page 7.

Upgrade Considerations

Update VM Properties

Rather than re-create 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 CCE components, update the properties of each VM to match the appropriate OVA, as follows:

1. Stop the VM.

2. Update the properties of each VM to match the properties of the appropriate OVA. Check the Virtualization for Packaged Contact Center Enterprise at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for descriptions of each OVA. Save your changes.

3. Restart the VM.

⚠️ Caution

Be careful when you upgrade the virtual machine network adapters. Done incorrectly, this upgrade can compromise the fault tolerance of your contact center.

For version-specific information on the VM properties in an OVA, Check the Virtualization for Packaged Contact Center Enterprise at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.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.

Self-signed Certificate for CCE Web Application

As part of the upgrade of CCE servers, self-signed certificates employed by CCE web applications like CCE web administration tool and Websetup, may get regenerated. You must add the new certificates to the trust list on the appropriate end devices.

Upgrade Tools

During the upgrade process, use the following tools as required:

- 12.5 ICM-CCE-Installer—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.

  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.

- 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.

  You can download the EDMT from Cisco.com by clicking Cisco Enhanced Data Migration Tool Software Releases.

  The prerequisites for running EDMT are:

  - EDMT also requires Microsoft® ODBC Driver 13 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015. The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the Prerequisites folder of EDMT

  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.

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 more information, see Silent Installation, on page 91.
Unified CCE Upgrade Overview

The supported upgrade paths to 12.5(1) are as follows:

- Release 12.0(x) to 12.5(1)
Common Ground Upgrade Process

- Packaged CCE 2000 Agents Deployment, on page 41
- Packaged CCE 4000 Agents Deployment, on page 56
- Packaged CCE 12000 Agents Deployment, on page 63

Packaged CCE 2000 Agents Deployment

Common Ground Upgrade Process

Redundant Upgrade Workflow

The redundant upgrade workflow is applicable to the solution deployments with Main site only.

Important

The upgrade requires four maintenance windows:

- First maintenance window to shut down services on Side A and upgrade Side A
- Second maintenance window in the middle of the upgrade to cut over from Side B to Side A. You must bring down Side B before you bring up Side A.
- Third maintenance window after you upgrade Side B to synchronize Side A to Side B.
- Fourth maintenance window to upgrade Cisco Unified Communications Manager (CUCM).

Common Preupgrade Tasks

Perform the tasks in the following table in the order that they are listed.
Preupgrade of Side A

**Task**

During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. Manually check the CTI Message Size counter in the Expanded Call Variable Payload List tool to ensure that the Default payload does not exceed the limit. If the Default payload exceeds the limit, modify it to meet the limit.

Take a snapshot of each virtual machine you are upgrading from the VMware vSphere Client.

Preupgrade of Side A

**Task**

Disable configuration changes on the Unified CCE. Change the following registry key to 1:

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance

Reverse the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority configuration so that calls are sent to the Side B Unified CVP server.

Using **Unified CCE Service Control**, stop all Unified CCE services on the Unified CCE servers that you are upgrading, and set the startup type to **Manual**.

1. Side A Unified CCE Logger
2. Side A Unified CCE AW-HDS-DDS
3. Side A PG
4. External HDS with Side A as the Central Controller preferred side (if used)

Verify that the services are stopped.

Upgrade Side A

Before you begin, check the following to confirm that call activity has ended on Side A:

- On the Unified CVP Statistics portal, make sure that no Side A ports are in use.
  1. Navigate to **Unified CCE Administration > Infrastructure > Inventory**.
  2. Click the **Statistics** icon to view the statistics for CVP machine.

  The **Infrastructure** tab for Call Server displays the port usage information.

- In the Unified Communications Manager RTMT tool, check that phones have migrated to Side B.

Place upgrade media ISOs on local data stores. Make sure to remove them when the upgrade is complete.
<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
</table>
| Upgrade to a supported version of ESXi version, if needed.  
For the supported ESXi versions for this release, see the Virtualization for Cisco Packaged CCE at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcee_virt_index.html.  
If you are using a supported ESXi version and want to upgrade to different supported ESXi version, you can upgrade now, or after the Packaged CCE upgrade is complete.  
See Upgrade VMware vSphere ESXi, on page 114. |
| Upgrade Unified CVP Server.  
| Upgrade all the Cisco Voice Gateways one after another.  
See Upgrade Cisco Voice Gateway IOS Version, on page 114.  
The IOS version of the Cisco Voice Gateways must be upgraded to the minimum version required by Packaged CCE 12.5(1). For more details, see the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information. |
| Upgrade all the Cisco Virtualized Voice Browsers one after another.  
| Upgrade the publishers/primary nodes of Cisco Finesse.  
| Upgrade the publishers/primary nodes of Cisco Unified Intelligence Center with Live Data and Identity Service (IdS).  
| Back up and export the Side A SQL database and the Outbound Option (if used) in Rigger VM.  
• Use Microsoft SQL Server Backup and Restore utilities for the back up.  
• Note the HDS customizable values.  
• Copy the backup files to a shared location. |
| Run the Enhanced Database Migration Tool on rigger, external HDS (if used), and non-external HDS to perform a schema upgrade during the upgrade process.  
See Run EDMT, on page 113. |
## Side A Postupgrade Tasks

### Task

If you use Outbound Option High Availability, for the enhancements in Outbound Option High Availability to work effectively, disable Outbound Option High Availability before the logger upgrade and then enable it after the upgrade. For details, see [Disable Outbound Options High Availability (If Applicable), on page 117](#).

Run the Unified CCE Release installer on the Side A Unified CCE logger.

See [Install Cisco Unified Contact Center Enterprise, on page 91](#).

Run the Unified CCE Release installer on the Side A Unified CCE AW-HDS-DDS.

See [Install Cisco Unified Contact Center Enterprise, on page 91](#).

Run the Unified CCE installer on the Side A PG.

See [Install Cisco Unified Contact Center Enterprise, on page 91](#).

(Optional) Upgrade the External HDS associated with Side A (if used)

Run the Unified CCE Release installer the External HDS associated with Side A.

See [Install Cisco Unified Contact Center Enterprise, on page 91](#).

(Optional) Upgrade ECE.


### Side A Postupgrade Tasks

You must bring down Side B before you bring up Side A. Perform these tasks during maintenance window to cut over from Side B to Side A.

### Task

Reverse the Cisco IOS Enterprise Ingress Voice Gateway dial-peer priority configuration so that calls are sent to the Side A Unified CVP server first and then to Side B.

(Optional) If you use Outbound Option High Availability, enable Outbound Option High Availability in the Web Setup tool. For details, see the Configure the Logger for Outbound Option topic in the [Outbound Option Guide for Unified Contact Center Enterprise](https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html).
**Task**

Using Unified CCE Service Control, stop all Unified CCE services on the Side B Unified CCE servers that you are upgrading, and set the startup type to **Manual**.

1. Side B Unified CCE Logger
2. Side B Unified CCE AW-HDS-DDS
3. Side B PG
4. External HDS with Side B as the Central Controller preferred side (if used)

Verify that the services have stopped.

Perform Database Performance Enhancement of TempDB, Logger Database, and AW-HDS Database. For more information, see **Database Performance Enhancement, on page 117, on page 140**.

Using Unified CCE Service Control, start all Unified CCE services on the Side A Unified CCE servers that you are upgrading, and set the startup type to **Automatic**.

1. Side A Unified CCE Logger
2. Side A Unified CCE AW-HDS-DDS
3. Side A PG
4. External HDS with Side A as the Central Controller preferred side (if used)

Verify that the services have started.

Set the following registry key to 0 on Side A Unified CCE Logger:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterA\Router\CurrentVersion\Configuration\Global\DBMaintenance
```

Direct agents to sign into the Side A Finesse Primary node.

---

**Preupgrade of Side B**

**Task**

Disable configuration changes on the Side B Unified CCE Logger. Change the following registry key to 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance name>\RouterB\Router\CurrentVersion\Configuration\Global\DBMaintenance
```

**Upgrade Side B**

Before you begin, check the following to confirm that call activity has ended on Side B:

- On the Unified CVP Statistics portal, make sure that no Side B ports are in use.

  1. Navigate to **Unified CCE Administration** > **Infrastructure** > **Inventory**.
  2. Click the **Statistics** icon to view the statistics for CVP machine.

    The **Infrastructure** tab for Call Server displays the port usage information.
In the Unified Communications Manager RTMT tool, check that phones have migrated to Side A. Place the upgrade media ISOs on local data stores. Ensure that you remove the media ISOs when the upgrade is complete.

<table>
<thead>
<tr>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upgrade to a supported version of ESXi version, if needed.</strong></td>
</tr>
<tr>
<td>For the supported ESXi versions for this release, see the <em>Virtualization for Cisco Packaged CCE</em> at <a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html</a>. If you are using a supported ESXi version and want to upgrade to different supported ESXi version, you can upgrade now, or after the Packaged CCE upgrade is complete. See <a href="#">Upgrade VMware vSphere ESXi</a>, on page 114.</td>
</tr>
<tr>
<td><strong>Upgrade the Unified CVP Reporting Server</strong></td>
</tr>
<tr>
<td>See <a href="#">Upgrade Unified CVP Reporting Server</a>, on page 114</td>
</tr>
<tr>
<td><strong>Upgrade Unified CVP Server.</strong></td>
</tr>
<tr>
<td><strong>Upgrade the subscribers/secondary nodes of Cisco Finesse.</strong></td>
</tr>
<tr>
<td><strong>Upgrade the subscribers/secondary nodes of Cisco Unified Intelligence Center with Live Data and Identity Service (IdS).</strong></td>
</tr>
<tr>
<td><strong>Back up and export the Side B SQL database and the Outbound Option (if used) database in the Rigger VM.</strong></td>
</tr>
<tr>
<td>• Use Microsoft SQL Server Backup and Restore utilities for the back up.</td>
</tr>
<tr>
<td>• Note the HDS customizable values.</td>
</tr>
<tr>
<td>• Copy the backup files to a shared location.</td>
</tr>
<tr>
<td><strong>Run the Enhanced Database Migration Tool on rigger, external HDS (if used), and non-external HDS to perform a schema upgrade during the upgrade process.</strong></td>
</tr>
<tr>
<td>See <a href="#">Run EDMT</a>, on page 113.</td>
</tr>
<tr>
<td>If you use Outbound Option High Availability, for the enhancements in Outbound Option High Availability to work effectively, disable Outbound Option High Availability before the logger upgrade and then enable it after the upgrade. For details, see <a href="#">Disable Outbound Options High Availability (If Applicable)</a>, on page 117.</td>
</tr>
</tbody>
</table>
Sync Side A to Side B

Perform these tasks during the third maintenance window to sync Side A and Side B.

**Task**

Set the following registry key to 0 on either the Side B Unified CCE Logger:

\[\text{HKEY_LOCAL_MACHINE}\backslash\text{SOFTWARE}\backslash\text{Cisco Systems, Inc.}\backslash\text{ICM}\backslash<\text{name}>\backslash\text{Router B}\backslash\text{Router}\backslash\text{CurrentVersion}\backslash\text{Configuration}\backslash\text{Global}\backslash\text{DBMaintenance}\]


On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change Startup to Automatic, in this order:

1. Side B Unified CCE Logger
2. Side B Unified CCE AW-HDS-DDS
3. Side B PG
4. External HDS with Side B as the Central Controller preferred side (if used)

Verify that the services are started.

---

Sync Side A to Side B

Perform these tasks during the third maintenance window to sync Side A and Side B.

**Task**

Set the following registry key to 0 on either the Side B Unified CCE Logger:

\[\text{HKEY_LOCAL_MACHINE}\backslash\text{SOFTWARE}\backslash\text{Cisco Systems, Inc.}\backslash\text{ICM}\backslash<\text{name}>\backslash\text{Router B}\backslash\text{Router}\backslash\text{CurrentVersion}\backslash\text{Configuration}\backslash\text{Global}\backslash\text{DBMaintenance}\]


On each of the following VMs, select **Unified CCE Service Control** on the desktop. Start the Unified CCE services and change Startup to Automatic, in this order:

1. Side B Unified CCE Logger
2. Side B Unified CCE AW-HDS-DDS
3. Side B PG
4. External HDS with Side B as the Central Controller preferred side (if used)

Verify that the services are started.
### Postupgrade Tasks

#### Task
Perform Database Performance Enhancement of TempDB, Logger Database, and AW-HDS Database for Side B. For more information, see Database Performance Enhancement, on page 117.

Run the **UserRoleUpdate.PS1** tool in Powershell in any one of the distributor machines. This ensures that the User Role is updated in the database for the existing users.

To download **UserRoleUpdate.PS1** script, go to the link [https://software.cisco.com/download/home/268439622/type](https://software.cisco.com/download/home/268439622/type) and select **UserRole Update Bulk Tool** from the list.

Download the file **UserRoleUpdateScript_1201.zip** and extract the script.

---

#### Postupgrade Tasks

#### Task
**Bring back Side A and Side B to call flow**


Change the Cisco IOS Enterprise Voice Gateway dial-peer configuration to point to both Side A and Side B Unified CVP Servers.

---

### Upgrade UCM in Side A and Side B

Perform these tasks to upgrade UCM in both Side A and Side B.

**Important**
Upgrade of CUCM requires a minimal maintenance window.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
</table>
| 1    | Upgrade the Side A CUCM Publisher and Subscriber.  
| 2    | Upgrade JTAPI on the Side A PG. See Upgrade Cisco JTAPI Client on the Unified Communications Manager PG, on page 116.  
**Important** If you are installing CUCM 12.5, install Cisco JTAPI Client on CUCM. See Install Cisco JTAPI Client on Unified Communications Manager, Release 12.0 and above, on page 115. |
Task Step

3. Upgrade the Side B CUCM Subscriber.
   **Important** The CUCM Publisher upgrade must be complete and the 12.5 software must be active before you upgrade the CUCM Subscriber.

   **Important** If you are installing CUCM 12.5, install Cisco JTAPI Client on the PG machine. For more information, see Install Cisco JTAPI Client on Unified Communications Manager, Release 12.0 and above, on page 115.

---

**UCM 12.5 Postupgrade Steps**

Perform these tasks if CUCM is on-box and you have upgraded to CUCM 12.5 on the M4 server. This procedure is performed on the main site.

---

**Note**

Ensure that you do not change IP address of the CUCM Publisher and Subscriber.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Move the CUCM Publisher and Subscriber from Side A host to a different host.</td>
</tr>
<tr>
<td>2</td>
<td>Move the CUCM Subscriber from Side B host to a different host.</td>
</tr>
<tr>
<td>3</td>
<td>Add CUCM Publisher as an external machine to the main site of the Packaged CCE Inventory.</td>
</tr>
</tbody>
</table>

---

**Multistage Upgrade Workflow**

---

**Note**

The multistage upgrade workflow is applicable for solution deployments with both main site and remote site (if available).

A 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 Packaged CCE 2000 Agent Deployments components, and the minimum component groupings that must occur together within each stage. Follow each
stage to completion within each 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.

Upgrade the CCE components as follows:

- Upgrade Agent Desktop, CUIC, Live Data, and IdS server along with the CCE Central Controller upgrade.
- Run Stage 3 and Stage 4 upgrades in the same maintenance window.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Gateways</td>
<td>• IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 6.) • IOS VXML Gateways • Cisco Virtualized Voice Browser</td>
<td></td>
</tr>
<tr>
<td>Stage</td>
<td>Component Group</td>
<td>Components</td>
<td>Notes</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------</td>
<td>------------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| 2     | Agent/Supervisor Desktop, Central Controller, and Reporting | • ECE  
• Cisco Finesse  
• Unified CCE Rogger  
• Admin & Data server (AW/HDS/DDS)  
• CUIC-LD-IDS  
• CUIC Reporting Templates | • After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs.  
• After you upgrade Finesse to Release 12.5, to load any gadgets to Finesse, you must first import all self-signed certificates (if applicable) to Finesse.  
• After you upgrade LD, you must import the Finesse certificate to LD. |
| 3     | Peripherals     | • Agent (Unified Communications Manager) PG  
• CTI Server  
• Outbound Option Dialer and SIP IOS Gateway | You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window. |
| 4     | Peripherals     | • MR PG, VRU PG  
• CRM connector | You can have many PGs located on different virtual machines. You can upgrade each PG virtual machine in its own maintenance window. |
| 5     | Call Processing | • Cisco Unified Communications Manager (Unified Communications Manager)  
• JTAPI on Agent (Unified Communications Manager) PG | You must install JTAPI client only when you upgrade to UCM 12.5.  
If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box. CUCM 12.5 on-box deployment are only supported for M5 servers.  
For more information, refer to *Virtualization for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html. |
Upgrade Flowcharts

The following diagram illustrates the solution-level upgrade flow for the Packaged CCE 2000 Agent Deployment solution upgrade.

Upgrade Flowcharts

The following diagrams illustrate the stages of the component-level upgrade flows for the Packaged CCE 2000 Agent Deployment 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 are required to perform.
Hardware Refresh with Common Ground Upgrade

If you are performing a hardware refresh as part of the upgrade process, you must first prepare the target servers as described in the following documents:

- Prepare Customer Site Servers, on page 5

After you configure the servers, you can move the VMs to the servers and complete the Common Ground Upgrade Process, on page 41.

As a part of hardware refresh, if you are migrating from existing C240 M3S/C240 M4SX to C240 M5SX/Specification based hardware, perform the following migration steps:

**Pre-migration Steps**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Update the annotation of the core VMs as per requirement for Specification Based hardware. See Installation Tasks, on page 15.</td>
</tr>
</tbody>
</table>

**Migration Steps**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Move the VMs to the target hardware</td>
</tr>
<tr>
<td>2</td>
<td>Log in to the Packaged CCE Administration and open the Inventory.</td>
</tr>
</tbody>
</table>
| 3     | Perform the following in the Packaged CCE Inventory:  
  1. Click Update Hosts.  
  2. Provide ESXI details of the target hardware.  
  3. Select the hardware type as **M5 Tested Reference Configuration/Specification Based Configuration**.  
  4. Complete the wizard.  
**Note** If CUCM and CVP Reporting Server were on-box in the old hardware, you must add them back as external machines after completing the deployment. |
Post-migration Step

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Complete the common ground hardware upgrade process. See Common Ground Upgrade Process, on page 41.</td>
</tr>
</tbody>
</table>

Packaged CCE 4000 Agents Deployment

Common Ground Upgrade Process

Multistage Upgrade Workflow

A 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 productionsystem to identify potential problems safely.

The following table details the required sequence for upgrading Packaged CCE 4000 Agent Deployments components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each 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.

Upgrade the CCE components as follows:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<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>ECE</td>
<td>After you upgrade Finesse to Release 12.5, to load any gadgets to Finesse, you must first import all self-signed certificates (if applicable) to Finesse.</td>
</tr>
<tr>
<td>2</td>
<td>Queuing and self-service</td>
<td>Cisco Unified Customer Voice Portal (CVP) (Reporting Server, Call Server/VXML Server, Unified Call Studio)</td>
<td>You must upgrade all sites before proceeding to the next stage.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Before you upgrade to Unified CVP 12.5, you must apply the latest ES of Packaged CCE 12.0.</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.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IOS VXML Gateways</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cisco Virtualized Voice Browser</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Reporting server</td>
<td>CUIC server</td>
<td>After you upgrade Cisco Unified Intelligence Center (CUIC), you must:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Enable CORS on the CUIC server, and add <code>cors allowed_origin</code> with the Finesse hostname.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Import LD and Finesse certificates to CUIC.</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>5</td>
<td>Central Controller</td>
<td>• Unified CCE Logger&lt;br&gt;• Admin &amp; Data server (AW/HDS/DDS)&lt;br&gt;• Standalone Live Data&lt;br&gt;• CUIC Reporting Templates&lt;br&gt;• Administration Client</td>
<td>• After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs.&lt;br&gt;• After you upgrade Live Data (LD), you must enable CORS on the LD box for Finesse and CUIC. For more information, see Installation and Upgrade Guide for Cisco Unified Intelligence Center Guide at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html">https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html</a>.&lt;br&gt;• After you upgrade LD, you must import the Finesse certificate to LD.</td>
</tr>
<tr>
<td>6</td>
<td>Peripherals</td>
<td>• Agent (Unified Communications Manager) PG&lt;br&gt;• CTI Server&lt;br&gt;• CTI OS Server&lt;br&gt;• Outbound Option Dialer and SIP IOS Gateway</td>
<td>• CTI OS Server is applicable only if Avaya PG is used.&lt;br&gt;• 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, VRU PG&lt;br&gt;• 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>• CTI OS is applicable only if Avaya PG is used.&lt;br&gt;• 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>
<tr>
<td>9</td>
<td>Call Processing</td>
<td>• Cisco Unified Communications Manager (Unified Communications Manager)&lt;br&gt;• JTAPI on Agent (Unified Communications Manager) PG</td>
<td>You must install JTAPI client only when you upgrade to UCM 12.5.&lt;br&gt;If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box. CUCM 12.5 on-box deployment are only supported for M5 servers.&lt;br&gt;For more information, refer to Virtualization for Packaged Contact Center Enterprise at <a href="https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html">https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html</a>.</td>
</tr>
</tbody>
</table>
Upgrade Flowcharts

The following diagram illustrates the solution-level upgrade flow for the Packaged CCE 4000 Agent Deployment solution upgrade.

The following diagrams illustrate the stages of the component-level upgrade flows for the Packaged CCE 4000 Agent Deployment 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 are required to perform.
Upgrade Flowcharts

A

Upgrade ECE

Upgrade Finesse

B

Upgrade CVP Reporting Server

Upgrade CVP Call Server/VXMLServer

Upgrade CVP Unified Call Studio

C

Cisco Virtualized Voice Browser

Upgrade Voice and Data Gateways

D
Version Upgrade

Upgrade Flowcharts

D

Upgrade CUIC Reporting Server

E

Live Data (if standalone)

E

Back up server registry, databases

F

Disable configuration changes
A 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 Packaged CCE 12000 Agent Deployments components, and the minimum component groupings that must occur together within each stage. Follow each stage to completion within each 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.

Upgrade the CCE components as follows:
## Multistage Upgrade Workflow

<table>
<thead>
<tr>
<th>Stage</th>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 3     | Gateways                         | • IOS Gateways (If used for ingress access only. If used for Outbound Option Dialer, see Stage 6.)  
• IOS VXML Gateways  
• Cisco Virtualized Voice Browser | |
After you upgrade Cisco Unified Intelligence Center (CUIC), you must:

- Enable CORS on the CUIC server, and add `cors allowed_origin` with the Finesse hostname.
- Import LD and Finesse certificates to CUIC.


### Stage 4

<table>
<thead>
<tr>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reporting server</td>
<td>CUIC server</td>
<td>After you upgrade Cisco Unified Intelligence Center (CUIC), you must:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Enable CORS on the CUIC server, and add <code>cors allowed_origin</code> with the Finesse hostname.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Import LD and Finesse certificates to CUIC.</td>
</tr>
</tbody>
</table>

### Stage 5

<table>
<thead>
<tr>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Controller</td>
<td>• Unified CCE Router</td>
<td>After you upgrade AW, import the self-signed certificate of all solution components (if applicable) to all AWs.</td>
</tr>
<tr>
<td></td>
<td>• Admin &amp; Data server (AW/HDS/DDS)</td>
<td>• After you upgrade LD, you must import the Finesse certificate to LD.</td>
</tr>
<tr>
<td></td>
<td>• Standalone Live Data</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CUIC Reporting Templates</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Administration Client</td>
<td></td>
</tr>
</tbody>
</table>

### Stage 6

<table>
<thead>
<tr>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripherals</td>
<td>• Agent (Unified Communications Manager) PG</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></td>
<td>• CTI Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• CTI OS Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Outbound Option Dialer and SIP IOS Gateway</td>
<td></td>
</tr>
</tbody>
</table>

### Stage 7

<table>
<thead>
<tr>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peripherals</td>
<td>• MR PG, VRU PG</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></td>
<td>• CRM connector</td>
<td></td>
</tr>
</tbody>
</table>

### Stage 8

<table>
<thead>
<tr>
<th>Component Group</th>
<th>Components</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<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>
You must install JTAPI client only when you upgrade to UCM 12.5.

If you upgrade to CUCM 12.5 on the M4 servers, ensure that you deploy CUCM off-box. CUCM 12.5 on-box deployment are only supported for M5 servers.

For more information, refer to Virtualization for Packaged Contact Center Enterprise at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html.

---

### Upgrade Flowcharts

The following diagram illustrates the solution-level upgrade flow for the Packaged CCE 12000 Agent Deployment solution upgrade.

[Diagram showing the upgrade flowchart]
The following diagrams illustrate the stages of the component-level upgrade flows for the Packaged CCE 12000 Agent Deployment 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 are required to perform.
Upgrade Flowcharts

D

Upgrade CUIC Reporting Server

Live Data

E

Back up server registry, databases

Disable configuration changes

F
Upgrade Flowcharts

G

Upgrade Unified Communications Manager

Upgrade JTAPI Client on Agent PG

End
Security Considerations

- Update the Java Runtime Environment (Optional), on page 71
- Upgrade Tomcat Utility, on page 72

**Update the Java Runtime Environment (Optional)**

The Unified CCE Installer installs the Java Runtime Environment (JRE) to a default location (for example, C:\Program Files (x86)\Java\jre<version>) and creates a JAVA_HOME environment variable set to that location. In most circumstances, you do not need to modify or configure the JRE.


If you have requirements for a different version of the JRE, you can update the JRE to a later version.

To update the JRE to a later version:

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

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

---

**Note**

- If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Ciscoapproved CA certificates in the java certificate store, and removes all the unapproved certificates.
- If you do not have CA certificates, import self-signed certificates of all components into AW machines. For more information, see Self-Signed Certificates section in the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

- Upgrade Tomcat to version 9.0 build releases. (That is, only version 9.0 build releases work with this tool.) You may choose to upgrade to newer builds of Tomcat release 9.0 to keep up with the latest security fixes.

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 9.0.21 to 9.0.22. 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 9.0.21 to 9.0.22, and then to 9.0.24, the utility reverts Tomcat to 9.0.22.

Before using the tool:


- Download the utility (UpgradeTomcatTool-&lt;version&gt;.jar) and copy it onto the Unified CCE component VMs.

  Download link: https://software.cisco.com/download/home/284360381/type/284416107/release.

- 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.

  Note

  Stop Unified CCE services on the VM before using the Tomcat Utility.
**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`

**Step 3**
When prompted, enter the full pathname of the new Tomcat installer. For example:
```
c:\tomcatInstaller\apache-tomcat-9.0.21.exe
```

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

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

---

**Revert Tomcat**

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

---

**Note**
Stop Unified CCE services on the VM before using the Tomcat Utility.

---

**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`

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

**Step 4**
Repeat these steps for all unified CCE component VMs.
Reference

- Tasks Common to Virtual Machines, on page 75
- Software Installations for Components, on page 82
- Common Software Upgrade Procedures, on page 113
- Simple Network Management Protocol, on page 120

Tasks Common to Virtual Machines

About Creating VMs

This chapter explains the sequence of tasks for creating virtual machines on each host server.

The sequence is:

1. Download the OVA files. See Open Virtualization Files, on page 75.
2. Create VMs.

Open Virtualization Files

Open Virtualization Format files define the basic structure of the VMs that are created—including the CPU, RAM, disk space, reservation for CPU, and reservation for memory.

1. Go to Download Software page on Cisco.com.
2. Select the required product release version.
3. Download and extract the file and save the OVAs to your local drive.
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 datastore where you uploaded the file.
6. Select the ISO file and click OK.

Unmount ISO File

Procedure

1. **Step 1** Right-click the virtual machine in the vSphere client and select Edit virtual machine settings.
2. **Step 2** Click Hardware and select CD/DVD Drive 1.
3. **Step 3** Select Client Device and click OK.

Create a Virtual Machine from the OVA

Before you begin

For information on VMs, see the following sections:

- About Creating VMs, on page 75
- Open Virtualization Files, on page 75
- Mount ISO Files, on page 76
### Procedure

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

**Step 2**  Right-click the Host and select **Deploy OVF Template**.

**Step 3**  Select an OVF template either by entering a URL or by browsing 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.

**Note**  For Cisco Unified CVP ova, an End User License Agreement displays. Click **Agree** and then click **Next**.

**Step 5**  Enter the virtual machine name. Click **Next**.

The name can contain up to 128 characters. Valid characters are period (.), hyphen (-), underscore (_), and alphanumeric. The first character must be alphanumeric.

The name can contain up to 32 characters. Invalid characters are space and special characters.

**Step 6**  On the Deployment Configuration page, use the drop-down to select the appropriate configuration. Then click **Next**.

**Step 7**  Choose a datastore on which to deploy the new virtual machine. Then click **Next**.

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

**Note**  If you are on a C240 M5SX server, remove the following annotations from the non-core component VMs: Cisco, Finesse, CUIC, and CVP.

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

**Step 8**
On the Disk Format page, keep the default virtual disk format: **Thick provisioned Lazy Zeroed format**. Click **Next**.

**Step 9**
Confirm that the Network Mapping page is correct for the Unified CCE Logger and PG:

a) For the Unified CCE Logger/Router/Logger/PG:
   - Map Public to UCCE Public Network  
   - Map Private to UCCE Private Network

b) For all other servers, map Public to UCCE Public Network.

**Step 10**
On the Network Mapping page, select the appropriate network from the **Destination** drop-down list.

**Step 11**
At the Successfully Completed message, click **Close**.

---

**Configure DNS Server**

This procedure is for Windows DNS server.

**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.
Procedure

Step 1 Log into the DNS server.
Step 2 In Windows, navigate to Administrative Tools > DNS. This opens the DNS Manager.
Step 3 In the Forward lookup zone, navigate to your deployment's domain name.
Step 4 Right-click the domain name and select New Host (A or AAAA).
Step 5 In the New Host dialog box, enter the computer name and IP address (IPv4) of VOS components.

Configure Database Drive

Note Complete this procedure to create a virtual drive, if the virtual drive was not automatically created in the VM.

Procedure

Step 1 Add a virtual drive as follows:

Using Web client:

a) Right-click the virtual machine and click Edit Settings.
b) On the Virtual Hardware tab, in New device section, select New Hard Disk.
c) Click Add.
d) Configure the required parameters as specified below:

Note Virtual machine templates for Logger, Rogger, AW, and HDS servers do not have a SQL database drive preprovisioned. The following reference table can be used to assign disk space to the virtual machine based on the type:

<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 custom size the SQL database disk space to meet data retention requirements, as calculated by the Database Estimator tool.

e) On the Disk Provisioning section choose Thick provision Lazy Zeroed format. Click Next.
f) Click OK to confirm the changes.
The Recent Tasks window at the bottom of the screen displays the progress.

**Step 2** Choose **Start > All Programs > Administrative Tools > Computer Management.**

**Step 3** In Windows, navigate to **Disk Management.**

**Step 4** Right-click on the **Disk 1** box and select **Online.**

**Step 5** Initialize Disk 1 as follows:
   a) Right-click on the **Disk 1** box and select **Initialize Disk.**
   b) Check the **Disk 1** checkbox.
   c) Select the **MBR (Master Boot Record)** radio button.
   d) Click **OK.**

**Step 6** Create a new disk partition as follows:
   a) Right-click the graphic display of **Disk 1** and select **New Simple Volume.**
   b) Click **Next** on the first page of the **New Simple Volume Wizard.**
   c) On the **Specify Volume Size** page, retain the default volume size. Click **Next.**
   d) On the **Assign Drive Letter or Path** page, assign drive letter (E). Click **Next.**
   e) On the **Format Partition** page, format the partition as follows:
      1. Select the **Format this volume with the following settings** radio button.
      2. Select **NTFS** from the **File system** drop-down menu.
      3. Select **Default** from the **Allocation unit size** drop-down menu.
      4. Enter a value in the **Volume label** field.
      5. Check the **Perform a quick format** checkbox.
      6. Click **Next.**
   f) Click **Finish.**

   The format is complete when the status changes to Healthy.

   A popup window displays a message that you need to format the disk before you can use it.

**Step 7** Format the disk.
   a) Click **Format disk.**
   b) Click **Start.**

   A popup displays a warning that formatting will erase all data on the disk.
   c) Click **OK.**
   d) When the format is complete, click **OK** to close the popup window.

---

**Install Antivirus Software**

Install one of the supported antivirus software products.

See the **Contact Center Enterprise Compatibility Matrix** at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for the list of supported products.
Important

Disable automatic updates. Update antivirus software manually.

Tip

To allow required access to installation program files or folders, perform file-blocking exclusions in the antivirus product file-and-folder protection rules. To do this in McAfee VirusScan:

1. Launch 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.

For more information about changing settings, see the documentation for your antivirus software.


Important

The firewall component of Symantec Endpoint Protection 12.1, the Network Threat Protection feature, must be disabled. If the feature remains enabled, which is the default, both sides of a duplexed router come up in simplex mode, thus blocking communication between each side of a router. This blocking impacts all deployment types.

Verification of the Downloaded ISO

Perform the following procedure to validate the downloaded ISO signed by Cisco, to ensure that it is authorized.

Procedure

Step 1
Install OpenSSL on Microsoft Windows.

Step 2
Add the OpenSSL installation path to System variables in the Environment Variables of the system.

Step 3
Add the downloaded ISO Image, ISO Image signature file and the Public key.der file in the same folder for the specific product component.

Step 4
Launch Command Prompt on the system.

Step 5
Run the following CLI (Command Line Interface) command to verify the files:

```
openssl dgst -sha512 -keyform der -verify <PUBLIC key.der> -signature <ISO Image.iso.signature> <ISO Image>
```

The system displays Verified OK on successful verification and Verification failed on verification failure.
Software Installations for Components

This section holds the consolidated list of software installation procedures that are referenced in the following section:

- Packaged CCE 2000 Agents Installation, on page 15
- Packaged CCE 4000 Agents Installation, on page 23
- Packaged CCE 12000 Agents Installation, on page 31

Install Microsoft Windows Server

Complete the following procedure to install Microsoft Windows Server on the virtual machines deployed.

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.

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 If prompted, enter the product key for Windows Server and click Next.

Step 6 Select the Desktop Experience option for the Windows Server 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.**

Microsoft Windows Server 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, refer to Microsoft documentation for details in installing Microsoft Windows Server Multilingual language packs.

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

**Related Topics**

*Mount ISO Files, on page 76*

---

**Install Microsoft SQL Server**

Install Microsoft SQL Server and store the SQL Server log and temporary files on the same vDisk as the operating system when using **default** (two) vDisk design. If you choose to use more than two virtual disks, then the tempDB cannot be on the same vDisk as the solution database.

For further information about the database placement and performance tuning the SQL installation, see the Microsoft documentation.

---

**Note**

For information about supported editions, see the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

---

**Before you begin**

**Note**

Microsoft SQL Server does not contain SQL Server Management Studio in the default toolkit. To rerun the SQL Server setup to install Management Studio, navigate to: **SQL Selection Center > Installation > Install SQL Server Management Tools.** If your computer has no internet connection, download and install SQL Server Management Studio manually.

VC++ 2017 build# 14.12.25810 is not compatible with the Cisco Contact Center Enterprise, ensure that it is not installed.

Add the virtual machine to a domain before installing SQL Server.
Procedure

Step 1  Mount the Microsoft SQL Server ISO image to the virtual machine. For more information, see Mount ISO Files, on page 76.

Step 2  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 3  On the Product Key page, enter the product key and then click Next.

Step 4  Accept the License Terms and then click Next.

Step 5  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 option, click Next on the Product Updates page.

Step 6  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 7  On the Feature Selection page, select only the following, and click Next:

- Database Engine Services
- Data Quality Services
- Data Quality Client
- Client Tools Connectivity
- Client Tools Backwards Compatibility
- Client Tools SDK
- SQL Client Connectivity SDK

Step 8  On the Instance Configuration page, select Default Instance and click Next.

Step 9  On the Server Configuration page, click the Services Account tab.

   a) Associate the SQL services with the virtual account.

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

   b) For the remaining services, accept the default values.

   c) In the Start Up Type column, for the SQL Server Agent service account, select Automatic from the list.

   d) Enable Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service.
ICM Installer automatically enables the **Grant Perform Volume Maintenance Task** for the NT service account, if it is not enabled automatically then you must enable **Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service** manually on the SQL server.

**Note**

On the **Server Configuration** page, click 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 database entry is related to the collation that you select. For example, if you set the collation for Latin1_General, but you select Chinese language at sign-in. When you enter field values in Chinese, the application displays the **unsupported character** error, because the database does not support the characters.

**Important** It is critical to select the correct collation setting for the language display on your system. If you do not select the correct collation during installation, you must uninstall and reinstall Microsoft SQL Server.

d) Check the **Binary** check box.

e) Click **OK**, and then click **Next**.

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) On the **TempDB** tab, set the **Initial size** and **Autogrowth** for Rogger, Logger, AW-HDS-DDS, AW-HDS, and HDS-DDS. For information about values for respective components, see **Increase Database and Log File Size for TempDB**, on page 86.

For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation.

e) Click **Next**.

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

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

Enable Named Pipes and set the sort order as follows:

a) Open the SQL Server 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 frees its memory when other processes request it, and it raises alerts about the memory monitoring tool.

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 SQL memory as 8GB and the minimum limit of the SQL memory as 4GB, using the **maximum memory usage** settings in the **SQL Server Properties** menu.

For more information about the SQL Server memory settings and its use, see the Microsoft SQL Server documentation.

**Step 15**  
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 Cisco Unified Contact Center Enterprise 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 16**  
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 17**  
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**.

**Related Topics**

- **Mount ISO Files**, on page 76

**Increase Database and Log File Size for TempDB**

To get the benefits of TempDB multiple data files support in CCE Components, Configure the following values as suggested for respective components.
Collation and Locale Settings for Localization

Microsoft SQL Server Collation Settings for Languages

You select a collation when you install Microsoft SQL Server, and it must be the collation that maps to the customer’s language display.

Remember

If your initial collation selection is incorrect, you must uninstall Microsoft SQL Server and reinstall it with the correct collation configuration.

For the languages supported by Packaged CCE and the SQL Server Collation setting for each language, see the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html.

Windows System Locale

The Windows system locale must match the display language; otherwise some characters appear incorrectly in the user interface and are saved incorrectly to the database. For example, if the system locale is English and you are working in Spanish, characters such as the acute a appear incorrectly.

Perform this procedure at both CCE Roggers, both CCE PGs, both CCE AWs, and any external HDS systems.

1. Open Control Panel > Clock, Language, and Region > Language.
2. Add the required language in the Change your language preferences page.
3. In the left pane, select Advanced settings.
4. Select the language for the Override for Windows display language option.
5. Select the language for the Override for default input method option.
6. Save your work and restart the virtual machine.

Install VMware Tools

Use this procedure to install and upgrade VMware tools from the VMware vSphere Client.

<table>
<thead>
<tr>
<th>CCE Component</th>
<th>vCPU</th>
<th>TempDB Data Files</th>
<th>TempDB Transaction Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Number of Files</td>
<td>Initial Size</td>
</tr>
<tr>
<td>Rogger</td>
<td>4</td>
<td>4</td>
<td>800MB</td>
</tr>
<tr>
<td>Logger</td>
<td>4</td>
<td>4</td>
<td>800MB</td>
</tr>
<tr>
<td>AW-HDS-DDS</td>
<td>4</td>
<td>4</td>
<td>800MB</td>
</tr>
<tr>
<td>AW-HDS</td>
<td>8</td>
<td>8</td>
<td>400MB</td>
</tr>
<tr>
<td>HDS-DDS</td>
<td>8</td>
<td>8</td>
<td>400MB</td>
</tr>
</tbody>
</table>
To install or upgrade VOS for Cisco Finesse, Cisco Unified Intelligence Center, and Cisco Unified Communications Manager:

1. Ensure that your virtual machine is powered on.
2. Right-click the VM in the virtual machine menu. Select Guest > Install / Upgrade VMware tools.
3. Choose the automatic tools update and press OK.

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

To install or upgrade VMs with Windows guest operating system:

1. Ensure that your Windows virtual machine is powered on.
2. Right click the VM in the virtual machine menu. Select Guest > Install / Upgrade VMware tools. Click OK on the popup window.
3. Log in to the VM as a user with administrative privileges.
4. Run VMware tools from the DVD drive.

   The installation wizard starts.
5. Follow the prompts in the wizard to complete the VMware Tools installation. Choose the Typical installation option.
6. When the VMware Tools installation has finished, restart the virtual machine for the changes to take effect.

When the process is complete, the tools are listed as Running (Current) on the VM's Summary tab in vSphere.

## Add Machine to Domain

### Add Machine to Domain Procedure

**Step 1** Navigate to Control Panel > System and Security > System.
**Step 2** Click Change Settings.
**Step 3** In the Computer Name tab, click Change.
**Step 4** Change the name of the computer from the name randomly generated during Microsoft Windows Server installation. The name does not contain underscores or spaces.
**Step 5** Select the Domain radio button to change the member from Workgroup to Domain.
**Step 6** Enter qualified domain name and click OK.
**Step 7** In the Windows Security dialog, enter the domain credentials and click OK.
**Step 8** On successful authentication, click OK.
**Step 9** Reboot the server and sign in with domain credentials.
Configure Network Adapters

The Unified CCE Logger, Router, Logger and the Unified CCE PG each have two network adapters. You must identify them by MAC address and Network Label, rename them, configure them, and set the interface metric value.

Procedure

Step 1 Identify the MAC addresses and labels for the network adapters as follows:
   a) From vSphere, select and right-click the VM.
   b) Select Edit Settings. In the Hardware tab, click Network adapter 1. In the right panel, write down the last few digits of MAC addresses and note whether the label is PCCE Public or PCCE Private. For example, Network adapter 1 may have a MAC address that ends in 08:3b and the network label PCCE Public.
   c) Repeat for Network adapter 2, noting its MAC address and label.
   d) From the VM console, type ipconfig/all from the command line. This displays the adapter names and physical addresses.
   e) Note the adapter names and physical addresses and match them with the MAC addresses and labels that you noted in VMware. For example, in ipconfig/all, Local Area Connection 2 may have a physical address that ends in 08-3b.
   f) Match the MAC address of the network adapter that VMware identified as PCCE Public with the corresponding physical address of Local Area Connector. In this example, the physical address of Local Area Connection 2 (08-3b) matches the MAC address (08-3b) of Network adapter 1. This means that Local Area Connection 2 is PCCE Public.

   Note Adapters may have a different name than Local Area Connection.

Step 2 Locate and rename the network adapters in Windows as follows:
   a) In Windows, open the Control Panel > Network and Sharing Center and click Change adapter settings.
   b) Right-click Local Area Connection and select Rename. Rename it to PCCE Public or PCCE Private, based on the matching you did above.
   c) Right-click Local Area Connection 2 and select Rename. Rename it to PCCE Public or PCCE Private, based on the matching you did above. In the example above, Local Area Connection 2 is renamed to PCCE Public.

Step 3 Set the Properties for PCCE Public as follows:
   a) Right-click PCCE Public and select Properties.
   b) In the Networking tab, uncheck Internet Protocol Version 6 (TCP/IPv6).
   c) Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
   d) In the General tab for Internet Protocol Version 4, select Use the following IP address and enter IP address, Subnet mask, Default gateway, and DNS servers.
   e) Click OK and Close to exit.

Step 4 Set the Properties for PCCE Private as follows:
   a) Right-click PCCE Private and select Properties.
   b) In the Networking tab, uncheck Internet Protocol Version 6 (TCP/IPv6).
   c) Select Internet Protocol Version 4 (TCP/IPv4) and click Properties.
   d) In the General tab for Internet Protocol Version 4, select Use the following IP address and enter IP address and Subnet mask.
e) Click **Advanced**.

f) Click the **DNS** tab and uncheck **Register this connection's addresses in DNS**.

g) In the **DNS server**, add a new A record that resolves to the private IP address. Also, create an associated pointer record for reverse lookups.

   **Note** For hostnames in A records, append the letter p to indicate that it is a private address.

h) Click **OK** to exit.

---

**Configure Network Adapter for Unified CCE AW-HDS-DDS, AW-HDS, HDS-DDS**

---

**Procedure**

**Step 1**  
Locate and rename the network adapter in Windows as follows:

a) In Windows, open the **Network and Sharing Center** and click **Change Adapter Settings**.

b) Right-click **Local Area Connection** and select **Rename**. Rename it to **UCCE Public**.

**Step 2**  
Set the Properties for **UCCE Public** as follows:

a) Right-click **UCCE Public** and select **Properties**.

b) In the Networking dialog box, uncheck Internet Protocol Version 6 (TCP/IPv6).

c) In the Networking dialog box, select Internet Protocol Version 4 (TCP/IPv4) and select **Properties**.

d) In the General dialog box for Internet Protocol Version 4, select **Use the following IP address** and enter the IP address, the Subnet mask, the default gateway, and DNS servers.

e) Click **OK** and **Close** to exit.

---

**Set Persistent Static Routes**

For geographically distributed Central Controller sites, redundant Rogger, logger, router, and Peripheral Gateway components typically have a Private IP WAN connection between Side A and Side B. Windows only allows one default gateway for each VM (which sends the Private Network traffic to the Public Network). So, you add a Static Route to all the VMs running the Rogger, logger, router, and PG applications.

To create a persistent static route with the **route add** command, you need the destination subnet, the subnet mask, the local gateway IP, and the interface number of the local Private Network interface:

```
route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p
```

You must launch the DOS prompt as an administrator to run the commands in this procedure.

---

**Procedure**

**Step 1**  
On each Rogger, router, logger, or PG VM, run **ipconfig /all**. Record the **IPv4 Address**, **Subnet Mask**, and **Physical Address** (MAC address) for the Private Network interface.
Step 2  On each of these VMs, run `route print -4`. Record the Interface for the Private Network. You can identify the correct interface by looking for its Physical Address (MAC address).

Step 3  On each of these VMs, run `route add <destination subnet> mask <subnet mask> <gateway IP> IF <interface number> -p` to add a persistent static route for the remote Private Network.

   On Side A VMs, use the gateway IP for Side B. On Side B VMs, use the gateway IP for Side A.

### Run Windows Updates

**Procedure**

Go to Settings > Update & Security and run Microsoft Windows Update.

### Install Cisco Unified Contact Center Enterprise

Install the Unified Contact Center Release 12.5 software on your Unified CCE virtual machines.

**Procedure**

**Step 1**  Login as a user with administrative privileges.

**Step 2**  Mount the Cisco Unified CCE ISO image to the virtual machine. See Mount ISO Files, on page 76.

**Step 3**  Run setup.exe from the D:\ICM-CCE Installer directory.

**Step 4**  Follow the InstallShield procedures to install Cisco Unified CCE.

**Step 5**  When the installation completes, restart the computer when prompted.

**Step 6**  Unmount the ISO image.

**Note**  If the ICM-CCE installer installs JRE on the Windows platform, the system retains only the Cisco approved CA certificates in the java certificate store, and removes all the unapproved certificates.

### 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 performed to run an installation wizard.

### Silent Installation Prerequisites

Before running a silent installation, complete the following tasks:

- Stop all applications that are running on the system.
• By default, silent installation assumes the following parameter: **Install on Drive C**.

To override this default, edit the ICMCCSilentsetup.ini file in the ICM-CCE-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 where the exported registry from source machine is placed.
  
  • To change the drive on which you are installing the application, change the `szDrive` parameter. Replace C with the drive where you want to install.
  
  • If you do not want to apply SQL Security Hardening, change the line that reads `szSQLSecurity=1` to `szSQLSecurity=0`.

---

**Note**

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

---

**Perform a Silent Installation**

**Procedure**

**Step 1**
Mount the Installation ISO image to the target machine. For more information, see Mount ISO Files, on page 76.

**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.

---

**Configure Permissions in the Local Machine**

In this release, Unified CCE defaults to providing user privileges by memberships to local user groups on local machines. This technique moves authorization out of Active Directory. However, it requires a one-time task on each local machine to grant the required permissions.
Configure Registry Permissions

This procedure only applies to distributor machines. Grant the required registry permissions for the `UcceConfig` group on the local machine.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Run the regedit.exe utility.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <code>HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM</code>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click and select Permissions.</td>
</tr>
<tr>
<td>Step 4</td>
<td>If necessary, add <code>UcceConfig</code> in <em>Group or user names</em>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select <code>UcceConfig</code> and check <em>Allow</em> for the <em>Full Control</em> option.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click <em>OK</em> to save the change.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Repeat the previous steps to grant Full Control to the <code>UcceConfig</code> group for <code>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, Inc.\ICM</code>.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Repeat the previous steps to grant Full Control to the <code>UcceConfig</code> group for <code>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2</code>.</td>
</tr>
</tbody>
</table>

Configure AW-HDS Database Permissions

Follow this procedure to grant access to the AWDB-HDS database to `UcceConfig` group members.

**Procedure**

In SQL Management Studio, do the following:

a) Go to Security > Logins.

b) Locate `<Machine name>\UcceConfig`. Right-click and select properties.

c) Go to User Mappings and select one AWDB database. Ensure that GeoTelAdmin, GeoTelGroup, and public are selected.

d) Repeat step c for the HDS database.

Configure Folder Permissions

Grant the required folder permissions to the `UcceConfig` group on the local machine.
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.


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. In the database size field, you can choose to retain the default value or enter a required value.
Step 6: Click OK to return to the Create Database dialog box.
Step 7: In the Add Device dialog box, click Log. Choose the desired drive. Retain the default value in the log size field and click OK to return to the Create Database dialog box.
Step 8: 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.


Configure Network Adapters for Cisco Unified CVP

Unified CVP has only one network adapter to configure. You must rename it and set its properties.
### Procedure

**Step 1** Navigate to **Control Panel > Network and Internet**.
**Step 2** Click **Network and Sharing Center**, and then click **Change adapter settings** in the left panel.
**Step 3** Right-click the adapter and select **Rename**. Change the name to UCCE Public.
**Step 4** Right-click UCCE Public and select **Properties**.
**Step 5** In the Networking dialog box, de-select Internet Protocol Version 6 (TCP/IPv6).
**Step 6** In the Networking dialog box, select Internet Protocol Version 4 (TCP/IPv4) and select **Properties**.
**Step 7** In the General dialog box for Internet Protocol Version 4, select **Use the following IP address** and enter the IP address, the Subnet mask, the default gateway and DNS servers.
**Step 8** Click **OK** and **Close** to exit.

### Install Cisco Unified CVP Server

**Procedure**

**Step 1** Log in to your system as a user with administrative privileges.
**Step 2** Mount the Unified CVP ISO image to the virtual machine. For more information, see **Mount ISO Files**, on page 76.
**Step 3** Run setup.exe from the D:\CVP\Installer_Windows directory.
**Step 4** Follow the InstallShield wizard to Run setup.exe from the D:\CVP\Installer_Windows directory:
   a) Accept the license agreement.
   b) In the **Select Packages** screen, check the type you are adding.
   c) Click **Next**.
   d) Choose U-Law encoded wave format.
   e) In the **Choose Destination Location** screen, accept the default. Click **Next**.
   f) In the **X.509 certificate** screen, enter the information that you want to include in the certificate.
   g) In the **Ready to Install** screen, click **Install**.
   h) Select the option to restart the computer after installation. Click **Finish**.
**Step 5** If Unified CVP Engineering Specials are available, copy them to the local drive. Follow the InstallShield wizard to install them.
**Step 6** Unmount the ISO image.

### Unified Customer Voice Portal Licenses

**Generate a License**

For instructions on generating Unified CVP licences, see the **Smart Licensing** section in Cisco Packaged Contact Center Enterprise Administration and Configuration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
Setup Unified CVP Media Server IIS

Procedure

**Step 1** Navigate to Start > Administrative Tools.

**Step 2** Choose Server Manager option navigate to Manage > Add Roles and Features.

**Step 3** Goto Installation Type tab, choose Role based or feature based installation option and click Next.

**Step 4** On Server Selection window, select server from the list and click Next.

**Step 5** Check Web Sever(IIS) check box to enable IIS and click Next.

**Step 6** No additional features are necessary to install Web Adaptor, click Next. Displays Web Server Role(IIS) tab.

**Step 7** Click Next. Displays Select Role Services tab.

**Step 8** Ensure that the web server components listed below are enabled.

- **Web Server**
  - Common HTTP Features
    - Default Document
    - Static Content
  - Security
    - Request Filtering
    - Basic Authentication
    - Windows Authentication
  - Application development
    - .NET Extensibility 4.6
    - ASP.NET 4.6
    - ISAPI Extensions
    - ISAPI Filters
  - Management Tools
    - IIS Management Console
    - IIS Management Compatibility
      - IIS6 Metabase Compatibility
    - IIS Management Scripts and tools
    - Management Service
Step 9: Click **Next**.
Step 10: Ensure that your settings are correct and click **Install**.
Step 11: After installation click **Close**.

### Related Topics
- Install FTP Server, on page 97
- Enable FTP Server, on page 97

### Install FTP Server

**Procedure**

1. Select **Start** > **Administrative Tools**.
2. Select **Server Manager** and click **Manage**.
3. Select **Add Roles and Features** and click **Next**.
4. In the **Installation Type** tab, select **Role-based or feature-based Installation** and click **Next**.
5. Select required server from the list and click **Next**.
6. On the **Server Roles** page, expand **Web Server (IIS)**.
7. On the **Server Roles** page, expand **Web Server (IIS)** and select **Internet Information Services (IIS) Manager**.
8. In the **Connections** panel:
   - Expand the CVP server to which you are adding the FTP site.
   - Right-click on **Site** and choose **Add FTP Site**.
9. Enter the **FTP Site Name**.
10. From the **Physical Path** field, browse to `C:\Inetpub\wwwroot` and click **Next**.
11. Choose **IP Address of CVP** from the drop-down list.
12. Enter the port number.
13. Select the **No SSL** check box and click **Next**.
14. Select the **Anonymous** and **Basic** check boxes in **Authentication** panel.

### Enable FTP Server

**Procedure**

1. Go to **Start** > **Programs** > **Administrative Tools** > **Server Manager**.
2. Expand **Roles** in the left panel of the **Server Manager** window.
3. Expand **Web Server (IIS)** and select **Internet Information Services (IIS) Manager**.
4. In the **Connections** panel:
   - Expand the CVP server to which you are adding the FTP site.
   - Right-click on **Site** and choose **Add FTP Site**.
5. Enter the **FTP Site Name**.
6. From the **Physical Path** field, browse to `C:\Inetpub\wwwroot` and click **Next**.
7. Choose **IP Address of CVP** from the drop-down list.
8. Enter the port number.
9. Select the **No SSL** check box and click **Next**.
10. Select the **Anonymous** and **Basic** check boxes in **Authentication** panel.
Step 11 Choose All Users from Allow Access To from the drop-down list.
Step 12 Select the Read and Write check box and click Finish.

---

**Configure Basic Settings for FTP Server**

**Procedure**

**Step 1** Navigate to the FTP server.
**Step 2** In the Actions tab, select Basic Settings.
**Step 3** Click Connect As.
**Step 4** Choose the Application User (pass-through authentication) option and click OK.
**Step 5** Click OK in Edit Site window.

---

**Install Cisco Unified CVP Reporting Server**

This task is required for the installation of the optional Unified CVP Reporting server.

The IBM Informix database server is installed as part of the Unified CVP Reporting Server.

Before installing the Unified CVP Reporting Server, you must configure a database drive. For more information, see Configure Database Drive, on page 79.

Complete the following procedure to install the Unified CVP Reporting server:

**Procedure**

**Step 1** Log in to your system as a user with administrative privileges.
**Step 2** Mount the Unified CVP ISO image to the virtual machine. For more information, see Mount ISO Files, on page 76.
**Step 3** Run setup.exe from the DVD drive located at the CVP\Installer_Windows directory.
**Step 4** Follow the InstallShield wizard to Run setup.exe from the D:\CVP\Installer_Windows directory:
   a) Accept the license agreement.
   b) In the Select Packages screen, check Reporting Server.
   c) In the Choose Destination Folder screen, select the folder location for the CVP installation folder.
   d) In the X.509 certificate screen, enter the information that you want to include in the certificate.
   e) In the Choose the database data and backup drive screen, enter the drive letter (typically, E).
   f) In the Database size selection screen, select Premium (438 GB).
   g) In the Ready to Install screen, click Install.
   h) Enter the Reporting Server password when prompted.
   i) Select the option to restart the computer after installation. Click Finish.
**Step 5** If Unified CVP Engineering Specials are available, copy them to the local drive. Follow the InstallShield wizard to install them.
Step 6  Unmount the ISO image.

What to do next
Repeat this procedure if your deployment requires a second, external Unified CVP Reporting Server.

Install Publishers/Primary Nodes of VOS-Based Contact Center Applications

This task is required for the publisher/primary nodes of the three VOS-based contact center applications: Cisco Cloud Connect, Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin
DNS Configuration is mandatory for installation of Cisco Cloud Connect, Cisco Unified Communications Manager, Cisco Unified Intelligence Center, Cisco Finesse and Cisco Identity Service (IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

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:
      • If you are installing Finesse or Unified Communications Manager, select OK.
      • If you are installing Unified Intelligence Center, select 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.
      • If you are installing Cloud Connect, select Cisco Contact Center Cloud Connect, and then select OK.
   d) In the Proceed with Install screen, select Yes.
   e) In the Platform Installation Wizard screen, select Proceed.
   f) In the Apply Patch screen, select No.
      Finesse does not have this step.
   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**.

Finesse does not have this step.

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**.

*Important* DNS client configuration is mandatory for Finesse. If you do not perform this step, agents cannot sign in to the desktop and you must reinstall Finesse.

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**.

*Important* Proper NTP configuration is essential.

s) In the **Security Configuration** screen, enter the security password and select **OK**.

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

Finesse does not have this step.

u) Unified Communications Manager only: On the **Smart Call Home Enable** screen, select **Disable All Call Home on System Start**.

v) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.

w) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and 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.

**Note** After successful installation of Cisco Unified Intelligence Center, import the stock templates.
Configure the Cluster for Cisco Unified Intelligence Center

**Procedure**

**Step 1** Direct a browser to the URL https://<hostname>:8443/oamp, where <hostname> is the hostname of your Cisco Unified Intelligence Center publisher.

**Step 2** Sign in using the system application user ID and password that you defined during installation.

**Step 3** From the section in the left, select **Device Configuration**.

**Step 4** Click **New**.

**Step 5** On the Device Configuration fields for the Subscriber, enter a name, the hostname or IP address or FQDN, and a description for the device.

*Note* All CUIC Subscribers must be entered here before you can install the software.

**Step 6** After you complete the cluster configuration, restart the publisher.

*Note* For 2000 Agents deployment, the system updates the Live Data failover settings.

---

**Unified Communications Manager License**


---

**Generate and Register License**

**Procedure**

**Step 1** Launch Unified Communications Manager in a browser (https://<IP Address of Unified CM Publisher>).

**Step 2** Click **Cisco Prime License Manager** and navigate to **Licenses > Fulfillment**.

**Step 3** Under **Other Fulfillment** options, click **Generate License Request**.

**Step 4** When the **License Request and Next Steps** window opens, copy the text (PAK ID).

**Step 5** Click the **Cisco License Registration** link.

**Step 6** Sign in and click **Continue to Product License Registration**.

**Step 7** In the **Enter a Single PAK or Token to fulfill** field, paste your PAK ID and click **Fulfill Single PAK/Token**.
You receive the license file in an email message.

### Install License

**Procedure**

- **Step 1**: Unzip the license file from the email message.
- **Step 2**: Under Other Fulfillment Options, select *Fulfill Licenses from File*.
- **Step 3**: Click *Browse* and locate your license file.
- **Step 4**: Click *Install* and close the popup window.
- **Step 5**: Navigate to *Product Instances*. Then click *Add*.
- **Step 6**: Fill in the name, hostname/IP address, username, and password for your Cisco Unified Communications Manager Publisher.
- **Step 7**: Select Product type of Unified CM.
- **Step 8**: Click *OK*.
- **Step 9**: Click *Synchronize Now*.

### Configure the Cluster for Cisco Unified Communications Manager

**Procedure**

- **Step 1**: Launch Unified Communications Manager Publisher in a browser (https://<IP Addr of CUCM Publisher>/ccmadmin).
- **Step 2**: Select *System > Server > Add New*.
- **Step 3**: On the Server Configuration page, select *CUCM Voice/Video* for the *Server Type*. Click *Next*.
- **Step 4**: On the Server Configuration page, enter the IP Address of the subscriber.
- **Step 5**: Click *Save*.

### Create a Unified Communications Manager AXL User Account

Create a Unified Communications Manager AXL user in Unified Communications Manager Administration. First create an Access Control Group with Standard AXL API Access, and then create an Application User with permission for that Access Control Group.
Procedure

Step 1  Launch Unified Communications Manager Administration in a browser (https://<IP Address of Unified Communications Manager Publisher>/ccmadmin).

Step 2  Create an Access Control Group, as follows:
   a) Navigate to User Management > User Settings > Access Control Group.
   b) Click Add New.
   c) Enter a name for the Access Control Group.
   d) Click Save.
      The Access Control Group Configuration page opens.
   e) From the Related Links drop-down menu, select Assign Role to Access Control Group and click Go.
   f) Click Assign Role to Group.
      The Find and List Roles popup window opens.
   g) Click Find.
   h) Check the Standard AXL API Access check box.
   i) Click Add Selected.
   j) Click Save.

Step 3  Create an Application User, as follows:
   a) Navigate to User Management > Application User.
   b) Click Add New.
   c) Enter a name and password for the Application User.
   d) In the Permissions Information section, click Add to Access Control Group.
      The Find and List Access Control Group popup window opens.
   e) Click Find.
   f) Check the check box for the Access Control Group you created.
   g) Click Add Selected.
   h) Click Save.

Configure the Cluster for Cisco Finesse

Procedure

Step 1  Launch the Cisco Finesse primary node in a browser (https://<FQDN of Finesse Primary node>/cfadmin).
If you are using an IPv6 client, you must include the port number in the URL (https://<FQDN of Finesse Primary node>:8445/cfadmin).

Step 2  Go to Home > Cluster Settings. (This path is based on the default configuration and assumes that you have not changed the page for the Cluster Settings gadget.)
Step 3 Add the hostname for the Cisco Finesse secondary node.

Step 4 Click Save.

Step 5 Restart Cisco Finesse Tomcat as follows:

a) To stop the Cisco Finesse Tomcat service, enter this CLI command: `utils service stop Cisco Finesse Tomcat`.

b) To start the Cisco Finesse Tomcat service, enter this CLI command: `utils service start Cisco Finesse Tomcat`.

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

This task is required for installation of the subscriber/secondary nodes of the three VOS-based contact center applications: Cisco Cloud Connect, Cisco Finesse, Cisco Unified Communications Manager, and Cisco Unified Intelligence Center.

Before you begin

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

Before you install the subscriber/secondary nodes, you must install the publisher/primary nodes and configure the clusters which include the subscriber's hostnames.

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, 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:

- If you are installing Finesse or Unified Communications Manager, select OK.

- If you are installing Unified Intelligence Center, select 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.

- If you are installing Cloud Connect, select Cisco Contact Center Cloud Connect, and 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**.

   Finesse does not have this step.

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**.

   Finesse does not have this step.

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

j) In the **DNS Client Configuration** screen, click **Yes** to enable DNS client.

   **Important**  DNS client configuration is mandatory for Finesse. If you do not perform this step, agents cannot sign in to the desktop and you must reinstall Finesse.

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**.

   Finesse does not have this step.

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.

   • For Cisco Unified Intelligence Center, you see a **Product Licensing** screen that shows the URL for obtaining the license and the Media Access Control (MAC) address. Write down the MAC address. You need this information for the license application.

   • The installation ends at a sign-in prompt.

Step 6  Unmount the ISO image.
Activate Services

Complete the following procedure to activate services.

Procedure

**Step 1**  Open Cisco Unified CM Administration at https://<IP Address of the CUCM Publisher>/ccmadmin.

**Step 2**  Select Cisco Unified Serviceability from the Navigation menu and click Go.

**Step 3**  Select Tools > Service Activation.

**Step 4**  From the Server drop-down list, choose the server on which you want to activate the service, and then click Go.

**Step 5**  For the Publisher, check the following services to activate and click Save:

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco Tftp
- Cisco Bulk Provisioning Service
- Cisco AXL Web Service
- Cisco Serviceability Reporter
- Cisco CTL Provider
- Cisco Certificate Authority Proxy Function
- Cisco Dialed Number Analyzer Server

**Step 6**  For the Subscribers, check the follow services to activate and click Save:

- Cisco CallManager
- Cisco IP Voice Media Streaming App
- Cisco CTIManager
- Cisco AXL Web Service
- Cisco CTL Provider
- Cisco Dialed Number Analyzer Server
Install the External HDS

Install and Configure the External HDS

The default deployment pulls data from the on-box AW-HDS-DDS database on the Unified CCE AW-HDS-DDS, where Real-time, Historical and Call Detail Data are stored.

If you need a longer retention period, you can optionally install the Administration Server, Real Time and Historical Data Server, Detail Data Server (AW-HDS-DDS) on a maximum of two separate, external servers. Each external server is configured as Central Controller Side A Preferred or Central Controller Side B Preferred.


Important

The External HDS (AW-HDS-DDS) must be able to connect to the Packaged CCE Side A and Side B ESXi hosts.


Follow this sequence of tasks to install an external HDS.

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Install Microsoft Windows Server, on page 82</td>
</tr>
<tr>
<td>2</td>
<td>Install Antivirus Software, on page 80</td>
</tr>
<tr>
<td>3</td>
<td>Install Microsoft SQL Server, on page 83</td>
</tr>
<tr>
<td>4</td>
<td>Install Cisco Unified Contact Center Enterprise, on page 91</td>
</tr>
<tr>
<td>6</td>
<td>Configure the database drive for the amount of data you want to keep. See Configure Database Drive, on page 79</td>
</tr>
<tr>
<td>7</td>
<td>Create an HDS Database for the External HDS, on page 108</td>
</tr>
<tr>
<td>8</td>
<td>Configure the External HDS, on page 108</td>
</tr>
<tr>
<td>9</td>
<td>Configure Unified Intelligence Center SQL User Account on the External HDS, on page 109</td>
</tr>
</tbody>
</table>
Create an HDS Database for the External HDS

Create the HDS database using ICMDBA.

Procedure

Step 1 Open Unified CCE Tools > ICMdba.

Note You must add instances to display in the ICMDBA. For more information, see Add a UCCE Instance, on page 110.

Step 2 Expand the instance tree view on the newly added external HDS until you can see your instance.

Step 3 Right click on the instance and select Create.

Step 4 In the Select component drop-down list, select Administration & Data Server and click OK.

Step 5 In the Select AW type drop-down list, select Enterprise and click OK.

Step 6 From the menu, select Database > Create. Click Add.

Step 7 Click the Data radio button, select the second disk drive, and enter the desired HDS size. Click OK.

Step 8 Click the Log radio button, select the second disk drive, and enter the desired log size. Click OK.

Step 9 Click Create.

Configure the External HDS

Procedure

Step 1 Open Unified CCE Web Setup.

Step 2 Choose 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) Click Small to Medium Deployment Size.
   c) Click Next.

Step 5 On the Server Role in a Small to Medium Deployment page, choose the option Administration Server Real-time and Historical Data Server, and Detail Data Server (AW-HDS-DDS). Click Next.

Step 6 On the Administration & Data Servers Connectivity page:
   a) Click the radio button for Primary Administration & Data Server.
b) In the *Secondary Administration & Data Server field, enter the hostname for the server.
c) In the *Primary Administration & Data Server field, enter the hostname for the server.
d) In the *Primary/Secondary Pair (Site) Name field, enter CCE-AW-1 for the first External HDS or CCE-AW-2 for the second External HDS.
e) Click Next.

Step 7 On the Database and Options page, configure as follows:
a) In the Create Database(s) on Drive field, choose C.
b) DO NOT click the Agent Re-skilling web tool. Packaged CCE does not support this tool. Supervisors reskill agents using the Agent tool in Unified CCE Administration.
c) Click Internet script editor.
d) Click Next.

c) Click Finish.

Configure Unified Intelligence Center SQL User Account on the External HDS

Procedure

Step 1 Launch Microsoft SQL Server Management Studio using the System Administrator login credentials.

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

This login is used 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 Click User Mapping.
a) Check the databases associated with the AWdb.
b) Choose each database and associate it with the db_datareader and public role, and click OK.

Step 5 Click OK.
Add a UCCE Instance

Procedure

Step 1  Launch Web Setup in the VM you want installed or upgraded.
Step 2  Sign in as a domain user with local administrator permission.
Step 3  Click Instance Management and then click Add.
Step 4  In the Add Instance dialog box, choose the customer facility and instance.
Step 5  In the Instance Number field, enter 0.
Step 6  Click Save.

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
```

Specifies the hostname or IP address of the Live Data secondary node.

Set IdS Subscriber Node

You must provide the publisher node the address of the subscriber node. You do this with the set ids subscriber command.

Procedure

Step 1  Log in to your publisher IdS node.
Step 2  Run the following command to set the subscriber node:

```
set ids subscriber name
```

Specifies the hostname or IP address of the IdS subscriber node address.
What to do next

You can use these Cisco IdS CLI commands only in an IdS standalone deployment. You run these commands on the IdS publisher node.

**Required Minimum Privilege Level:** Ordinary

Use this command to show IdS subscriber node information.

```
show ids subscriber
```

There are no required parameters.

**Required Minimum Privilege Level:** Advanced

Use this command to unset IdS subscriber node configuration.

```
unset ids subscriber
```

There are no required parameters.

Install Enterprise Chat and Email

Enterprise Chat and Email (ECE) is an optional feature that provides chat and email functionality to the contact center. In Packaged CCE 2000 Agents deployment, you can deploy ECE Data Servers on-box for up to 400 agents. Deploy ECE off-box for up to 1500 agents. You can also deploy the ECE Data Servers on a separate server. On-box installation is supported on the B200 M4, C240 M4SX and C240 M5SX hardware only.

---

**Note**

Core servers and external servers support ECE high availability.

- ECE Data Server can be deployed on both Side A and Side B.
- ECE Data Servers can be deployed as external machines.

---

Deploy the ECE Web Server on an external server. You can place that server either in the same data center as the ECE Data Server or in a DMZ if customer chat interactions require that.

Use OVA file to create a virtual machine for an on-box ECE. For information about creating a virtual machine, see Create a Virtual Machine from the OVA, on page 76.

ECE 12.5 does not support the archive database. While upgrading from ECE 12.0 to 12.5 in a PCCE 2000 agent deployment, if you choose to refer to the old archive database, keep a copy of the archive database off the PCCE box. For more information, see the Planning Database Upgrade from SQL 2014 to SQL 2016 section in the Enterprise Chat and Email Installation Guide (for Packaged Contact Center Enterprise) at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

Install Cisco Virtualized Voice Browser

Cisco Virtualized Voice Browser (Cisco VVB) provides a platform for interpreting VXML documents. Cisco VVB serves as an alternative to the use of IOS Voice Browsers (VXML gateways). When an incoming call arrives at the contact center, Cisco VVB allocates a VXML port that represents the VoIP endpoint. Cisco VVB sends HTTP requests to the Unified CVP VXML server. The Unified CVP VXML server executes the request and sends back a dynamically generated VXML document.


Install the Language Pack

If a customer requires a language other than the default (English), download the Packaged CCE Language Pack executable from the Unified Contact Center Download Software page.

Install Language Pack

Install the Language Pack on the AW machine and on any External HDS servers after upgrading them.

After you install the Language Pack, the Unified CCE Administration Sign In page has a language drop-down menu that lists all available languages. Select a language to display the user interface and the online help in that language.

Uninstall Language Pack

You can uninstall the Language Pack from Windows Control Panel > Programs and Features > Uninstall or change a program.

Set Cloud Connect Secondary Node

Use the set cloudconnect subscriber command to provide the address of the secondary node in the primary node.

Procedure

Step 1  Sign in to your primary Cloud Connect node.
Step 2  Run the following command to set the secondary node:

```
set cloudconnect subscriber {name}
```

name

Specifies the FQDN or IP address of the Cloud Connect subscriber node (maximum 255 characters).
Initial Configuration for Cloud Connect in 4000 and 12000 Agents

Before adding Cloud Connect to the inventory, you will have to install the certificates from both Cloud Connect publisher and subscriber.


**Procedure**

**Step 1**
In Unified CCE Administration, navigate to **Infrastructure Settings > Inventory**.

**Step 2**
Select the site and in the External Machines section, click the + icon.

**Step 3**
In the Add Machine dialog box:

- a) Select **Cloud Connect Publisher** from the Type list.
- b) Enter Hostname or IP Address of the Cloud Connect Publisher Node.
- c) Enter Username and Password for your Cloud Connect cluster Administrator.
- d) Click **Save**.

Common Software Upgrade Procedures

Run EDMT

**Before you begin**

- EDMT requires Microsoft® ODBC Driver 13 for SQL Server® and Visual C++ Redistributable for Visual Studio 2015. The latest version of these packages can be downloaded from the Microsoft website. However, a copy of the same is also available in the Prerequisites folder of EDMT.
- 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.
- The installer, not the EDMT, upgrades the AW database for the Administration & Data Server.

**Procedure**

**Step 1**
Launch EDMT.exe.

**Step 2**
In the Cisco Unified ICM/Contact Center Enterprise Enhanced Database Migration Tool that appears, click **Next**.

**Step 3**
Under **Migration Type**, click the **Common Ground** radio button and then click **Next**.

**Step 4**
In the **Warning** dialog box that appears, click **Yes**.

**Step 5**
From the **Authentication** drop down list, choose either **Windows Authentication** or **SQL server Authentication**.
Step 6  Click **Refresh Database List**, and select the database you want to migrate from that list.

Step 7  Click **Next**.

Step 8  Click **Start Migration**.

**Note**  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. 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.

Step 9  Click **Exit** after the data migration is complete.

**Note**  Set the TempDB AutoGrowth of Data files to 100 MB manually.

---

**Upgrade VMware vSphere ESXi**

If you use VMware vCenter Server in your deployment, upgrade VMware vCenter Server before upgrading VMware vSphere ESXi.

Upgrade VMware vSphere ESXi on Side A and Side B servers to the latest version supported with this release of Packaged CCE. Packaged CCE uses standard upgrade procedures, which you can find using VMware documentation (https://www.vmware.com/support/pubs/).

**Upgrade Unified CVP Reporting Server**


**Upgrade Cisco Voice Gateway IOS Version**

Perform this procedure for each gateway on the side you are upgrading.

Upgrade the Cisco Voice Gateway IOS version to the minimum version required by this release. See the *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html for IOS support information.

**Procedure**

**Step 1**  Copy the new image from the remote TFTP server into flash memory, making sure that you specify your own TFTP server's IP address and Cisco IOS filename.

**Step 2**  Verify that the new image was downloaded.

**Step 3**  Boot using the new image. Update the gateway config to boot using the new version.

**Step 4**  Reload the gateway to use the new image.
Install Cisco JTAPI Client on Unified Communications Manager PG

After setting up the Cisco Unified Communications Manager (CUCM) PG, you must install the Cisco JTAPI client. PG uses Cisco JTAPI to communicate with CUCM. Install the Cisco JTAPI client from CUCM Administration.

Note

Continue with the steps provided in this section if you are installing the JTAPI client for CUCM version earlier than Release 12.0.

To install the JTAPI client for CUCM, Release 12.0 and above, see Install Cisco JTAPI Client on Unified Communications Manager, Release 12.0 and above, on page 115.

Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

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 while 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. Download the JTAPI plugin file.

Step 6
Choose Save and save the plugin 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.

Step 12
Reboot the machine.

Install Cisco JTAPI Client on Unified Communications Manager, Release 12.0 and above

Complete the following procedure only if you are installing JTAPI client to connect to Cisco Unified Communications Manager, Release 12.0 and above.
Before you begin

Before you install the JTAPI client, ensure that the previous version is uninstalled.

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 while 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. Download the JTAPI plugin file.
Step 6  Choose Save and save the plugin file to a location of your choice.
Step 7  Unzip the JTAPI plugin zip file to the default location or a location of your choice.

There are two folders in the unzipped folder, CiscoJTAPIx32 and CiscoJTAPIx64.
Step 8  Run the install32.bat file in the CiscoJTAPIx32 folder.
Make a note of the default location where the installer installs the JTAPI client.
Step 9  To accept the default installation path, click Enter and proceed.
Follow the instructions. Click Enter whenever necessary as per the instructions.
Provide IP address of the TFTP server, when prompted for. For 4000 and 12000 deployments, IP address should be same as CUCM IP address provided in CUCM PIM.
The JTAPI client installation completes at the default location. The following message is displayed:

Installation Complete.

Step 10 Reboot the machine.

What to do next

Note

The default location, where the JTAPI client is installed, also contains the uninstall32.bat file. Use this file to uninstall this version of the client, if necessary.

Upgrade Cisco JTAPI Client on the Unified Communications Manager PG

If you upgrade Unified Communications Manager (Unified CM) in the contact center, also upgrade the JTAPI client that resides on the Unified CM 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.

To install the JTAPI client for the Unified CM release that you have upgraded to, see the Install Cisco JTAPI Client on Unified Communications Manager PG, on page 115 topic.

**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.

### Disable Outbound Options High Availability (If Applicable)

Perform the following steps on Side A:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Launch <a href="#">Websetup</a>. Navigate to <a href="#">Component Management</a> &gt; <a href="#">Loggers</a>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Edit the <a href="#">Logger</a> and navigate to <a href="#">Additional Options</a>. Uncheck <a href="#">Enable High Availability</a> under <a href="#">Outbound Option</a> and click <a href="#">Next</a>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enable <a href="#">Stop and then start(cycle) the Logger Service for this instance (if it is running)</a> checkbox. Click <a href="#">Next</a> to complete the setup.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Repeat similar steps (steps 1, 2, and 3) for side B.</td>
</tr>
</tbody>
</table>

### 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 TempDB**

Perform this procedure on Logger, Rigger, AW-HDS-DDS, AW-HDS and HDS-DDS machines to get the benefits of TempDB features for SQL Server. For more information about the SQL Server TempDB Database and its use, see the Microsoft SQL Server documentation for TempDB Database.

**Note**

This procedure applies to the Common Ground upgrade process only.

**Procedure**

| Step 1 | Use [Unified CCE Service Control](#) to stop the Logger and Distributor services. |
Step 2  Login to SQL Server Management Studio and run the following queries on the master database.

- To modify the existing TempDB Initial size to the recommended value:
  
  ```sql
  ALTER DATABASE tempdb MODIFY FILE
  (NAME = 'tempdev', SIZE = 800, FILEGROWTH = 100)
  ALTER DATABASE tempdb MODIFY FILE
  (NAME = 'templog', SIZE = 600, FILEGROWTH = 10%)
  ```

- To add multiple TempDB files:

  ```sql
  USE [master];
  GO
  ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev2', FILENAME = N'<SQL Server TempDB path>', SIZE = 800, FILEGROWTH = 100);
  ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev3', FILENAME = N'<SQL Server TempDB path>', SIZE = 800, FILEGROWTH = 100);
  ALTER DATABASE [tempdb] ADD FILE (NAME = N'tempdev4', FILENAME = N'<SQL Server TempDB path>', SIZE = 800, FILEGROWTH = 100);
  GO
  ```

Note  

- For example,

  ```sql
  <SQL Server TempDB path> = C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA\tempdev2.ndf
  ```

- Make sure that you modify the values in the query based on the machines. For more information, see Increase Database and Log File Size for TempDB, on page 86.

Step 3  Restart the SQL Services.

Step 4  Start the Logger and Distributor services.

Performance Enhancement of Logger Database

Perform this procedure on Side A and Side B of the Logger database.

Procedure

Step 1  Use the Unified CCE Service Control to stop the Logger service.

Step 2  From the command prompt, run the `RunFF.bat` file which is located in the `<SystemDrive>:\icm\bin` directory.

Step 3  Proceed with the application of fill factor to ICM databases.

Note: Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes anywhere between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>\temp\<DatabaseName>_Result.txt`.

Step 4  Use the Unified CCE Service Control to start the Logger service.

Troubleshooting Tips

See the `RunFF.bat/help` file for more information.
**Performance Enhancement of AW-HDS Database**

**Procedure**

**Step 1** Use the Unified CCE Service Control to stop the Distributor service.

**Step 2** From the command prompt, run the `RunFF.bat` file which is located in the `<SystemDrive>:\icm\bin` directory.

**Step 3** Proceed with the application of fill factor to ICM databases.

*Note:* Based on the size of the database, it takes several minutes to several hours to apply fill factor to the database. For example, it takes between 2 to 3 hours for a 300-GB HDS. After the process is completed, the log file is stored in `<SystemDrive>\temp\<DatabaseName>_Result.txt`.

**Step 4** Use the Unified CCE Service Control to start the Distributor service.

**Troubleshooting Tips**

See the `RunFF.bat/help` file for more information.

---

**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**.

**Reduce Reserved Unused Space for HDS**

Enable trace flag 692 on HDS database server to reduce the growth of reserved unused space on the AW-HDS, AW-HDS-DDS, HDS-DDS database servers, after you upgrade or migrate to Microsoft SQL 2017. For more information about the trace flag 692, see the Microsoft Documentation.

**Procedure**

Run the following command to enable trace flag 692 on HDS database server:

```
DBCC TRACEON (692, -1);
GO
```
An increase in the unused space may lead to unexpected purge trigger in HDS, trace flag 692 helps in mitigating this unexpected purge issue. After you enable the trace flag, there will be an increase of 10% to 15% CPU for a short duration.

**Simple Network Management Protocol**

Simple Network Management Protocol (SNMP) facilitates the exchange of management information among network devices so that administrators can manage network performance and solve network problems. SNMP community strings, users, and network destinations are configured in Cisco Unified Serviceability.

Unified Serviceability is one of the tools that open from the Navigation drop-down in Cisco Unified Communications Solutions tools. You can also access Unified Serviceability by entering http://x.x.x.x/ccmservice/, where x.x.x.x is the IP address of the publisher.


**Community Strings**

The SNMP agent uses community strings to provide security. You must configure community strings to access any management information base (MIB). Add new community strings in the Cisco Serviceability Administration interface.

A community string is configured with:

- a server
- a name of up to 32 characters
- a setting to accept SNMP packets from any host or from specified hosts
- access privileges (readonly, readwrite, readwritenotify, notifyonly, readnotifyonly, and none)
- a setting to apply the community string to all nodes in the cluster

**Notification Destinations**

Add notification destinations for delivery of SNMP notification events when events occur. Add and maintain notification destinations in the Cisco Serviceability Administration interface.

A notification destination is configured with:

- a server
- the host IP addresses of the trap destination
- a port number
- the SNMP version (V1 or V2c)
- the community string name to be used in the notification messages that the host generates
• the notification type

• a setting to apply to the notification destination configuration to all nodes in the cluster