Reference

- Tasks Common to Virtual Machines, on page 1
- Software Installations for Components, on page 8
- Common Software Upgrade Procedures, on page 43
- Simple Network Management Protocol, on page 50

Tasks Common to Virtual Machines

About Creatings 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 1.
2. Create VMs .
3. After you create all the VMs, perform initial configuration. See the **Post Installation Configuration** 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.

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 **Datastore**.
2. Select the datastore that will hold the ISO file.
3. Right click and select **Browse datastore**.
4. Click the **Upload files** button.
5. Browse to the location on your local or network drive where you saved the ISO file, and upload the ISO to the datastore.

Note After copying the ISO to the target machine for installation or upgrade, right-click on the ISO file and check its properties before mounting. Ensure that the ISO is not marked as blocked, else select the unblock box and click **Apply**.

Mount the ISO image:

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

Unmount ISO File

Procedure

Step 1 Right-click the virtual machine in the vSphere client and select **Edit virtual machine settings**.
Step 2 Click **Hardware** and select **CD/DVD Drive 1**.
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 Creatings VMs, on page 1
- Open Virtualization Files, on page 1
- Mount ISO Files, on page 2

Procedure

Step 1 Select the host in the vSphere client.

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

Step 3 On the **Select an OVF template** page, browse to the location on your local drive where you stored the OVA. Click **Open** to select the file. Click **Next.**

Note
For Cisco VVB OVA, an End User License Agreement displays. Click **Agree** and then click **Next**.

Step 4 On the **Select a name and folder** page, enter a name for the virtual machine and then choose the location for the virtual machine.

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

Step 5 Click **Next**.

Step 6 On the **Select a compute resource** page, select the destination compute resource. Click **Next.**

Step 7 On the **Review details** page, verify the OVF template details.

Step 8 On the **Configuration** page, select the applicable configuration from the available list. Click **Next**.

Note
When deploying a CUIC OVF, choose **Co-Resident** for a 2000 Agent Deployment and **Stand-Alone** for a 4000 Agent and 12000 Agent Deployment.

Step 9 On the **Select storage** page, ensure that the virtual disk format is **Thick provision Lazy Zeroed** and then choose a datastore on which you want to deploy the new virtual machine. Click **Next.**

For each datastore, the following tables describe the RAID group, the ESXi Host, and the virtual machines for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX servers.

Note
If you are on a Cisco UCS C240 M5SX or Cisco UCS C240 M6SX server, remove the following annotations from the non-core component VMs: Cisco, Finesse, CUIC, and CVP.

RAID configuration for the Cisco UCS C240 M4SX, Cisco UCS C240 M5SX, and Cisco UCS C240 M6SX

RAID Group	VM Datastore	ESXi Host	Virtual Machines
VD0	datastore 1	A	ESXi operating system Unified CCE Rogger Side A Unified CCE Router Side A Unified CCE Logger Side A Unified Communications Manager Publisher Cisco Finesse Primary
VD1	datastore 2	A	Unified CCE AW-HDS-DDS Side A
VD2	datastore 3	A	Unified Communications Manager Subscriber 1 Unified CVP Server Side A
VD3	datastore 4	A	Unified Intelligence Center Server Publisher Unified CCE PG Side A
VD0	datastore 1	B	ESXi operating system Unified CCE Rogger Side B Unified CCE Router Side B 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 10 On the **Select networks** page, confirm that the network mapping is correct for the Unfied CCE Rogger and PG:

a) For the Unifed CCE Rogger/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 11 On the **Ready to complete** page, click **Finish** to create the VM.

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 requires FQDNs in order to work properly.

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 in to 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) In the **Virtual Hardware** tab, click on **Add New Device**.
c) You can select the type of device you wish to add. Select **Hard Disk**. The new hard disk appears. Assign the desired disk space to the hard disk.
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 must be used to assign disk space to the virtual machine based on the type of validation errors will occur:

Virtual Machine Template	Default Second Disk Size
Logger	500 GB
Rogger	150 GB
AW-HDS-DDS	500 GB
AW-HDS	500 GB
HDS-DDS	500 GB

You can custom size the SQL database disk space to meet data retention requirements on an external AW-HDS-DDS server only, as calculated by the Database Estimator tool.

e) On the **Disk Provisioning** section, choose **Thick provision Lazy Zeroed**.
f) In the **VM Options** > **Advanced Options** section, retain the default options.
g) Click **OK** to confirm the changes.

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

Step 2 In Windows, navigate to **Disk Management**.

Step 3 Right-click on the **Disk 1** box and select **Online**.

Step 4 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 5 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. Click **Format Disk**.
3. Select File System as **NTFS** and click **Start**.
4. Select **Default** from the **Allocation unit size** drop-down menu.

5. Enter a value in the **Volume label** field.
6. Check the **Perform a quick format** checkbox.
7. Click **Next**.

f) Click **Finish**.

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

The format is complete when the status changes to Healthy.

Step 6 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.

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.

For more information on security guidelines, refer the **General Antivirus Guidelines** section in the *Security Guide for Cisco Unified ICM/Contact Center Enterprise Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

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:

Procedure

	Command or Action	Purpose
Step 1	Launch the VirusScan console.	

	Command or Action	Purpose
Step 2	Right-click **Access Protection** and select **Properties**.	
Step 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.

Verification of the Downloaded ISO or Minor Release Installer

Perform the following procedure to validate the downloaded ISO or Minor Release Installer 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 or Minor Release Installer, ISO Image signature file or Minor Release Installer 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 or Minor Release Installer.exe.signature> <ISO
Image or Minor Release Installer exe>
```

The system displays `Verified OK` on successful verification and `Verification failed` on verification failure.

Note
If the verification fails do not proceed with the installation, contact Cisco Support for a valid ISO or Minor Release Installer.

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
- Packaged CCE 4000 Agents Installation
- Packaged CCE 12000 Agents Installation

Install Microsoft Windows Server

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

Note Deploying VM with Guest Operating System 'Microsoft Windows Server 2019' on ESXi 7.0 using CCE OVA template displays a warning message "The configured guest OS (Microsoft Windows Server 2016 or later (64-bit)) for this virtual machine does not match the guest that is currently running (Microsoft Windows Server 2019 (64-bit)). You should specify the correct guest OS to allow for guest-specific optimization". This warning message is informational only and has no detrimental effect on the system. This warning message is displayed only once and can be dismissed.

Note Before installing 12.5(1) ICM on SQL Server 2019, make sure to install ODBC Driver 13 for SQL Server® manually.

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 Install VMWare tools. See Install VMware Tools, on page 15.

Step 12 Open the **Network and Sharing Center**, and in the View your basic network info and set up connections section, click **Ethernet**.

Step 13 In the Ethernet Status window, click **Properties**.

Step 14 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**.

Edge Chromium (Microsoft Edge) is not installed by default on the Windows server. To install Edge Chromium (Microsoft Edge), see *Microsoft* documentation.

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 2

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 2.

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**
- **Client Tools Connectivity**
- **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.

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

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

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**.

Note

Unified 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.

Step 10 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**.

Step 11 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 Increase Database and Log File Size for TempDB, on page 14.

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

e) On the **MaxDOP** tab, choose the value of MaxDOP as half the value of logical CPU cores detected on the computer which is displayed just above the MaxDOP configuration. For example, if the logical CPU cores are detected as 4, then MaxDOP should be configured as 2.

Note
SQL Server installation automatically recommends the MaxDOP server configuration based on the number of processors available. This feature is introduced in SQL Server 2019 and later. In SQL Server 2017, you can configure MaxDOP post installation. To configure MaxDOP, do the following:

1. In **Object Explorer**, right-click the database instance and select **Properties**.
2. Select **Advanced**.
3. In the **Max Degree of Parallelism** box, configure the number of processors as recommended above.

f) Click **Next**.

Step 12 On the **Ready to Install** page, click **Install**.

Step 13 On the **Complete** page, click **Close**.

Step 14 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. Named Pipes
   2. 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 and minimum limit of the SQL memory using the **maximum memory usage** settings in the **SQL Server Properties** menu as shown below:

Component	SQL Server Minimum Memory	SQL Server Maximum Memory
Logger	2GB	4GB
Rogger	2GB	3GB
AWS-HDS	4GB	8GB
AWS-HDS=DDS	4GB	8GB
HDS-DDS	4GB	8GB

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 2

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.

CCE Component	vCPU	TempDB Data Files			TempDB Transaction Log File	
		Number of Files	Initial Size	Autogrowth	Initial Size	Autogrowth
Rogger	4	4	800MB	100MB	600MB	10MB
Logger	4	4	800MB	100MB	600MB	10MB
AW-HDS-DDS	4	4	800MB	100MB	600MB	10MB
AW-HDS	8	8	400MB	100MB	600MB	10MB
HDS-DDS	8	8	400MB	100MB	600MB	10MB

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.

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

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 Rogger, 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.

Step 5 Assign an interface metric value for the network adapter:

a) Select the network adapter and right-click **Properties**.
b) In the **Networking** tab, select the appropriate Internet Protocol version and click **Properties**.
c) In the **Internet Protocol Version Properties** dialog box, click **Advanced**.
d) In the **IP Settings** tab, uncheck the **Automatic metric** checkbox and type a low value in the **Interface metric** text box.

Note
A low value indicates a higher priority. Make sure that the Public Network card should have a lower value compared to the Private Network card.

By default, the value of the Interface Metric property for a network adapter is automatically assigned and is based on the link speed.

e) Click **OK** to save the settings.

Repeat the steps to assign an interface metric value for the internal/private cluster communication network adapter.

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.

Note Before installing 12.5(1) ICM on SQL Server 2019, make sure to install ODBC Driver 13 for SQL Server® manually.

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 2.

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 for Unified CCE Release 12.5(1)

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 SQL Security Hardening should not be applied as part of silent installation on Windows Server 2019 and SQL Server 2019 platform. Change the line that reads szSQLSecurity=1 to szSQLSecurity=0. SQL Security Hardening can be applied post installation using Security Wizard tool.

Perform a Silent Installation for Unified CCE Release 12.5(1)

Procedure

Step 1 Mount the Installation ISO image to the target machine. For more information, see Mount ISO Files, on page 2.

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

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

Installation starts. Upon successful installation, the server reboots.

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

Silent Installation Prerequisites for Unified CCE Release 12.6(2)

Before running a silent installation, complete the following tasks:

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

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

Perform a silent installation for Unified CCE Release 12.6(2)

Procedure

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

Example:

```
"c:\ICM12.6(2).exe" /r /f1c:\myanswerfilename.iss
```

The /r flag is for recording the response file.

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

Note
There is no space between the /f1 and the start of the file path. If no /f1 flag is present, the response file is written to a default location (C:\Windows)".

When you have navigated through the setup process (which completes a full installation of the product on the machine recording the response file) the resulting response file can be copied to any additional machine during a silent installation.

Step 2 Run setup from a command prompt using the same syntax as listed in step 1, with one exception: use **/s** instead of **/r** to indicate the install should run silently using the response file found at /f1filepath.

Example:

```
"c:\ICM12.6(2).exe" /s /f1c:\myanswerfilename.iss /f2c:\silentinstall.log
```

The /f2 flag creates a log file.

What to do next

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

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

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.

Note You can use the ADSecurityGroupUpdate registry key to choose between the new default behavior and the previous behavior. For more information, see the chapter on solution security in the Solution Design Guide.

Before using the Configuration Manager tool, configure the required registry and folder permissions for the `UcceConfig` group.

Configure Registry Permissions

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

Procedure

Step 1 Run the `regedit.exe` utility.

Step 2 Select `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM`.

Step 3 Right-click and select **Permissions**.

Step 4 If necessary, add `UcceConfig` in **Group or user names**.

Step 5 Select `UcceConfig` and check **Allow** for the **Full Control** option.

Step 6 Click **OK** to save the change.

Step 7 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, Inc.\ICM`.

Step 8 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinSock2`.

Note
If you have configured the Unified CCE Administration Client, open Local security policy and go to **User Rights Assignment**. Right click **Create Global Object**. Go to **properties** and add the local Group `UcceConfig`.

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 netbios 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.

Note SQL login account `<Machine netbios name>\UcceConfig` is created during CCE installation on the machine. If there is any change in the machine hostname, the SQL login account has to be deleted and re-created with the new **machine netbios name**.

Configure Folder Permissions

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

Procedure

Step 1 In Windows Explorer, select `<ICM install directory>\icm`.
Step 2 Right-click and select **Properties**.
Step 3 On the **Security** tab, select `UcceConfig` and check **Allow** for the **Full Control** option.
Step 4 Click **OK** to save the change.
Step 5 Repeat the previous steps to grant **Full Control** to the `UcceConfig` group for `<SystemDrive>:\temp`.

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.

Note
Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

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**.

For more information about configuring Outbound Options, see the *Outbound Option Guide for Unified Contact Center Enterprise* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html

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 2.

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) On the **Voice Prompt Encode Format** screen, select the codec according to your requirement.
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 featue 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 26
Enable FTP Server, on page 27

Install FTP Server

Procedure

Step 1 Select **Start** > **Administrative Tools**.

Step 2 Select **Server Manager** and click **Manage**.

Step 3 Select **Add Roles and Features** and click **Next**.

Step 4 In the **Installation Type** tab, select **Role-based or feature-based Installation** and click **Next**.

Step 5 Select required server from the list and click **Next**.

Step 6 On the **Server Roles** page, expand **Web Server (IIS)**.

Step 7 Check **FTP Server** and click **Next**.

Step 8 On the **Features** page, click **Next**.

Step 9 On the **Configuration** page, click **Install**.

Enable FTP Server

Procedure

Step 1 Go to **Start** > **Programs** > **Administrative Tools**> **Server Manager**.

Step 2 Expand **Roles** in the left panel of the **Server Manager** window.

Step 3 Expand **Web Server (IIS)** and select **Internet Information Services (IIS) Manager**.

Step 4 In the **Connections** panel:

a) Expand the CVP server to which you are adding the FTP site.

b) Right-click on **Site** and choose **Add FTP Site**.

Step 5 Enter the **FTP Site Name**.

Step 6 From the **Physical Path** field, browse to `C:\Inetpub\wwwroot` and click **Next**.

Step 7 Choose **IP Address of CVP** from the drop-down list.

Step 8 Enter the port number.

Step 9 Select the **No SSL** check box and click **Next**.

Step 10 Select the **Anonymus** 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.

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

Before you begin

IBM Informix database server 12.10 FC3 is installed as part of the Unified CVP Reporting Server.

- Only the actual Local Administrator (should not be renamed) of this system can install CVP Reporting Server.
- Ensure that Unified CVP Reporting Server is not part of any domain and is part of a work group.

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 2.

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://<hostmame>: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

Note From Release 12.0 onwards, Cisco Smart Licensing replaces Cisco Prime License Manager. To use Cisco Smart Licensing, create and configure a Smart Account before you upgrade or migrate the Unified Communications Manager server. For more information, see **Licensing** section in *Installation Guide for Cisco Unified Communications Manager and IM and Presence Service*, at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-guides-list.html.

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

Note 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.
   - 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

Note You must not exceed the maximum number of AW-HDS-DDS that the design permits for the corresponding deployment type.

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**.

For more information about retention, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.

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

Refer to 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 for external HDS server requirements.

Follow this sequence of tasks to install an external HDS.

Sequence	Task
1	Install Microsoft Windows Server, on page 9
2	Install Antivirus Software, on page 7
3	Install Microsoft SQL Server, on page 10
4	Install Cisco Unified Contact Center Enterprise, on page 19
5	Configure SQL Server for CCE Components. Refer 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.
6	Configure the database drive for the amount of data you want to keep. See Configure Database Drive, on page 5
7	Create an HDS Database for the External HDS, on page 38
8	Configure the External HDS , on page 39
9	Configure Unified Intelligence Center SQL User Account on the External HDS, on page 40

Sequence	Task
10	Configure Unified Intelligence Center Data Sources for External HDS. Refer 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.
11	If you have an IPv6 enabled deployment, configure a Forward lookup AAAA record for the External HDS in DNS. Refer to the Configure DNS for IPv6 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.

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 40.

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**.

Note
Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

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

Note
Ensure that there is enough free space in the hard disk (at least 20% of database size) to accommodate the log growth.

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, configure as follows:

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

a) Choose the current instance.
b) Choose the deployment type as **Enterprise**.
c) Choose the deployment size as **Small to Medium**.
d) Click **Next.**

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

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.**

Step 8 On the **Central Controller Connectivity** page, configure as follows:

a) For Router Side A, enter the IP Address of the Unified CCE Rogger A.
b) For Router Side B, enter the IP Address of the Unified CCE Rogger B.
c) For Logger Side A, enter the IP Address of the Unified CCE Rogger A.
d) For Logger Side B, enter the IP Address of the Unified CCE Rogger B.
e) Enter the Central Controller Domain Name.
f) Click **Central Controller Side A Preferred** or **Central Controller Side B Preferred** .
g) Click **Next.**

Note
The Administration & Data Server can connect to the central controller with a hostname of maximum 24 characters.

Step 9 Review the **Summary** page, and then 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*
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*
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.

Note Packaged CCE requires that the **Context Root Name** is set to **system** while installing ECE. Setting **Context Root Name** to any name other than **system** will result in integration failure between Packaged CCE and ECE. **Context Root Name** can only be set while installing ECE, reinstalling ECE is required to change it.

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 2.

ECE 12.0 doesn't support the archive database. While upgrading from ECE 11.6 to 12.0 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.

For capacity information, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise*, available at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-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 runs the request and sends back a dynamically generated VXML document.

Cisco VVB is installed on box. Installation and configuration procedures are documented in the *Installation and Upgrade Guide for Cisco Virtualized Voice Browser* at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/products-installation-guides-list.html.

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 Subscriber or Secondary Node of Cloud Connect

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).

Common Software Upgrade Procedures

Run EDMT

Before you begin

- 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.

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

You cannot upgrade CVP Reporting Server from 12.0 to 12.6 because the version of IBM Informix database server has changed. You need to uninstall CVP Reporting Server 12.0 and install CVP Reporting Server 12.6 . For more details, see the **Upgrade Unified CVP Reporting Server** section in the *Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html.

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.

For more information, see https://www.cisco.com/c/en/us/td/docs/routers/access/1900/software/configuration/guide/Software_Configuration/upgrade.pdf.

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 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 12.5.

To install the JTAPI client for CUCM, Release 12.5 and above, see Install Cisco JTAPI Client on PG, on page 46.

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**.We recommend you to download the 64 bit version. However, if you have already downloaded the 32 bit version, you can proceed to step 7.

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 PG

Complete the following procedure only if you are installing JTAPI client to connect to Cisco Unified Communications Manager, Release 12.5 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 Client for Windows** 64 bit or **Download Cisco JTAPI Client for Windows** 32 bit.

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 `CiscoJTAPIx64` and `CiscoJTAPIx32`.

Step 8 Run the `install64.bat` file in the `CiscoJTAPIx64` folder or run the `install32.bat` file in the `CiscoJTAPIx32` folder.

The default install path for JTAPI client is `C:\Program Files\JTAPITools`.

Step 9 To accept the default installation path, click Enter and proceed.

Follow the instructions. Click Enter whenever necessary as per the instructions.

Note
Starting from Cisco Unified Communications Manager (CUCM) 12.5 SU4 and 14.0 (or any other service updates thereafter) on these release trains, only 64-bit version of the JTAPI client is supported on the Agent PG.

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 `uninstall64.bat` and `uninstall32.bat` file. Use this file to uninstall this version of the client, if necessary.

Upgrade Cisco JTAPI Client on PG

If you upgrade Unified Communications Manager (Unified CM) in the contact center, also upgrade the JTAPI client that resides on the 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 PG, on page 45 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

Step 1 Launch **Websetup**. Navigate to **Component Management** > **Loggers**.

Step 2 Edit the **Logger** and navigate to **Additional Options**. Uncheck **Enable High Availability** under **Outbound Option** and click **Next**.

Step 3 Enable **Stop and then start(cycle) the Logger Service for this instance (if it is running)** checkbox . Click **Next** to complete the setup.

Step 4 Repeat similar steps (steps 1, 2, and 3) for side B.

Database Performance Enhancement

After you perform a Common Ground or a Technology Refresh upgrade, complete the procedures described in this section 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, on page 48 (You can skip this when performing a Technology Refresh upgrade)

- Performance Enhancement of Logger Database, on page 49
- Performance Enhancement of AW-HDS Database, on page 49

Performance Enhancement of TempDB

Perform this procedure on Logger, Rogger, 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.

Note If the Performance Enhancement of TempDB procedure is already completed on Unified CCE 12.5(1) or 12.6(1), then do not repeat the same procedure upon upgrading to Unified CCE 12.6(2).

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 primary database.

- To modify the existing TempDB Initial size to the recommended value:

```
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:

```
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 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 14.

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 `<ICM install directory>:\icm\bin` directory.

Step 3 Proceed with the application of fill factor to Unified 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 `<ICM install directory>:\icm\bin` directory.

Step 3 Proceed with the application of fill factor to Unified 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 and Logger

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 and Logger database, after you upgrade or migrate to Microsoft SQL 2017 or 2019. 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 and Logger database:

```
DBCC TRACEON (692, -1);
GO
```

Note
An increase in the unused space may lead to unexpected purge trigger in HDS and Logger, 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. If the trace flag needs to be retained, the server startup options has to be updated using the -T(upper case) option. For more information, see https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/database-engine-service-startup-options?view=sql-server-ver15.

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.

See the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html for information about configuring SNMP for Unified CCE.

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

Reference