Configure Customer Instance

Configure Customer Instance for the 2000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 2000 agent for Cisco HCS for CC for Contact Center.

Table 1: Create customer instance for 2000 agent deployment of Cisco HCS for CC for Contact Center

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 2	
2	Set Up Virtual Machine Startup and Shutdown, on page 2	
3	Create a Domain Controller Server, on page 3	
4	Configure Cisco Unified CCE Rogger, on page 6	
5	Configure Unified CCE AW-HDS-DDS, on page 16	
6	Configure Unified CCE PG, on page 22	
7	Configure Unified CVP, on page 34	
8	Configure Cisco IOS Enterprise Voice Gateway, on page 52	
9	Configure Unified Communications Manager, on page 58	
10	Configure Unified Intelligence Center Coresident Deployment, on page 65	

Sequence	Task	Done?
11	Configure Cisco Finesse, on page 79	

Upgrade VMware Tools

Procedure

Step 1 Right-click on the VM. Select **Guest** > **Install / Upgrade VMware tools**.

Step 2 Wait for the popup window (this may take time) and accept the default Automatic Tools Upgrade.

Step 3 Click **OK**.

Step 4 Restart, only if you are prompted.

Note VMWare Tools must be installed and up to date in all VMs.

Set Up Virtual Machine Startup and Shutdown

Procedure

Step 1 In the **VMware vSphere Client** window, select **ESXi server**.

Step 2 Click the **Configuration** tab.

Step 3 Click the **Virtual Machine Startup/Shutdown** link.

Step 4 Click **Properties**.

Step 5 In the **Virtual Machine Startup and Shutdown** dialog box, check the **Allow virtual machines to start and stop automatically with the system** check box.

Step 6 Use the **Move Up** and **Move Down** buttons to rearrange the virtual machines under **Automatic Startup** in the following order:

- Cisco Unified CCE Central Controller Servers
- Cisco Unified CCE Administration and Data Servers
- Cisco Unified CCE PG Servers
- Cisco Unified CVP Servers
- Cisco Finesse Servers
- Cisco Unified Intelligence Center
- Cisco Unified Communication Manager
- Cisco Unified CVP Reporting Server
- Cisco Unified CVP OAMP Server

Step 7 Click **OK**.

Create a Domain Controller Server

Create a Virtual Machine for the Domain Controller

Procedure

Step 1 Create a new virtual machine from vCenter.

Step 2 On the **Name and Location** page, provide a name for the **Domain Controller**.

Step 3 In the **Disk format** field, choose the **Thick Provisioned** format.

Step 4 Enter the virtual machine specifications, see *Domain and Active Directory Considerations for HCSCC* section of *Solution Design Guide for Cisco Hosted Collaboration Solution for Contact Center* http://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html.

Install Antivirus Software

Perform this procedure for both golden-template and for direct-install options.

Install any of the antivirus software products supported by HCS for CC for Contact Center.

For more information on the anitvirus software and versions supported by HCS for CC for Contact Center, see *Contact Center Enterprise Compatibility Matrix* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-device-support-tables-list.html.

Install any of the antivirus software products supported by Enterprise Chat and Email. For more information on the anitvirus software and versions supported by Enterprise Chat and Email, see the *System Requirements for Enterprise Chat and Email* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-implementation-design-guides-list.htm.

Important Update antivirus software, manually - do not enable automatic updates.

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

- Launch the VirusScan console.
- Right-click **Access Protection**, then select **Properties**.
- In the **Anti-virus Standard Protection** category, make sure that the Prevent IRC communication check box is unchecked in the **Block** column.

Important HCS for CC for Contact Center supports Symantec Endpoint Protection.

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

If you retain the default (enabled) start services on side A and B of the router, a Symantec message pops up in the system tray indicating: The client will block traffic from IP address [side A router address] for the next 600 seconds(s). This message also appears in the client management security log. The Symantec Network Threat Protection traffic log indicates that a default firewall rule called “Block_all” was dynamically enabled. The result in both sides of the router come up in simplex mode.

To avoid the issue, you must disable the **Symantec** firewall and restart both sides of the router. To do this, double click the Symantec icon in the system tray and select **Change Settings**. Then configure settings for Network Threat Protection and uncheck the **Enable Firewall** check box at the top of the Firewall tab.

Disabling Port Blocking

On computers that run Unified CVP Server components, such as Call Server and Reporting server, which has an anti-virus software configured to block ports, exclude Unified CVP processes and `tomcat6.exe`. In addition, exclude Voice Browser.exe for the call server process.

Note If you use an anti-virus software other than McAfee Virus Scan, perform the equivalent exclusions in port blocking rules for that software.

Procedure

Step 1 Launch **McAfee**.

Step 2 In the **VirusScan Console**, double-click **Access Protection**, then choose **Anti-virus Standard Protection**.

Step 3 Choose **Prevent IRC communication** from the list, then click **Edit**.

Step 4 Add `tomcat6.exe`, `tomcat5.exe`, `VoiceBrowser.exe` to the **Processes to Exclude** , then click **Ok**.

Step 5 Click **Ok**.

Enable DNS Server

Procedure

Step 1 Go to **Start** > **Server Manager**.

Step 2 In the **Server Manager** window, select **Manage** > **Add Roles and Features**.

Step 3 In the **Before You Begin** tab, click **Next**.

Step 4 In the **Installation Type** tab, choose **Role based or feature based installation** option and click **Next**.

Step 5 The **Server Selection** tab, displays the list of servers that are running on Windows Server. Select a server from this list and click **Next**.

Step 6 On the **Server Roles** tab, do the following:

a) Select the **Active Directory Domain Services** if you intend to promote a domain controller.

b) In the **Add Features that are required for Active Directory Domain Services?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AS LS Tools
      - [Tools] AS DS Snap-Ins and Command-Line Tools
      - [Tools] Active Directory Administrative Center

Step 7 Select **DNS Server**.

Step 8 In the **Add Features that are required for DNS Server?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DNS Server Tools

Step 9 In the **Features** tab, ensure **Remote Server Administration Tools and Role Administration Tools** are selected and click **Next**.

Step 10 In the **AD DS** tab, click Next.

Step 11 In the **DNS Sever** tab, click Next.

Step 12 n the **Confirmation** tab, click Install.
The **Result** tab displays the progress of the DNS server installation.

Step 13 After the installation completes, click on the **Promote this server to a domain controller** link to make the server a domain controller.

Step 14 In the **Deployment Configuration** tab, select **Add a New Forest,** enter a valid fully qualified domain DNS name, and click **Next**.

Note Enter a valid domain name that adheres to the naming conventions listed at https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

Step 15 In the **Domain Controller Options** tab, enter the following and click **Next**:

a) From the **Forest functional level** drop-down list, select Windows Server version based on your AD version.

b) From the **Domain functional level** drop-down list, select Windows Server version based on your AD version.

Note You can also choose to set the forest functional level to an older Windows Server version.

However, the Windows Server 2012 forest functional level does not provide any new functionality over the Windows Server 2008 R2 forest functional level.

c) Ensure that the **Domain Name System (DNS) Server** and the **Global Catalog (GC)** check box is checked.

d) Set the **Directory Services Restore Mode** password.

Step 16 In the **Additional Options** tab, enter the **NetBios** name and click **Next**.

Step 17 In the **Paths** tab, enter the paths where you would like to store the database, log files, and SYSVOL.

Step 18 In the **Review Options** tab, click **Next**.

Step 19 In the **Prerequisites Check** tab, you can read through the warning if any and click **Install**.
The **Results** page displays whether the installation was a success. The server will automatically reboot in 10 minutes.

Configure a DNS Server

To configuring a DNS server, see Configure DNS Server, on page 109.

Create Two-Way Forest Trust

To create two-way forest trust between Unified CCE and CCDM,

Configure Cisco Unified CCE Rogger

This table lists the configuration procedures you must perform to configure Cisco Unified CCE Rogger.

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Verify the Machine in Domain, on page 9	
3	Configure the Domain Manager, on page 10	
4	Configure Unified CCE Encryption Utility, on page 11	
5	Configure SQL Server for CCE Components, on page 11	
6	Allocate a Second Virtual Hard Drive, on page 12	

Sequence	Task	Done?
7	Configure the Unified CCE Logger, on page 12	
8	Configure the Unified CCE Router, on page 15	
9	Load Base Configuration, on page 16	
10	Verify Cisco Diagnostic Framework Portico, on page 31	
11	Cisco SNMP Setup, on page 31	

Configure Network Cards

Note Do this for all the Unified CCE virtual machines that have two network adapters.

Procedure

Step 1 Navigate to **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
Step 2 Click **Change adapter settings** to open the Network Connections page.
Step 3 Rename the network adapter with Visible IP address configurations as **Visible**.
Step 4 Rename the network adapter with Private IP address configurations as **Private**.
Step 5 On the **Network Connections** page, press **Alt N** to display the Advanced menu.
Step 6 From the **Advanced** menu, select **Advanced Settings**.
Step 7 Under **Adapters and Bindings**, sort the connections so that `visible` is on top.
Step 8 Click **OK**.

Configure Private Ethernet Card

Procedure

Step 1 Right-click **private** and select **Properties**.
Step 2 Uncheck **Client for Microsoft Networks**.
Step 3 Uncheck **File and Printer Sharing for Microsoft Networks**.
Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.
Step 5 Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.
a) Remove the IP Address for the Default Gateway.
b) Remove the IP Address for the Preferred DNS server.
c) Remove the IP Address for the Alternate DNS server.
Step 6 Click the **Advanced** button. Open the DNS tab. Uncheck **Register this connection's addresses in DNS**.

Step 7 Add an entry for the private IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "p" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAp" for the private IP address.

Step 8 Optional: Add another entry for the private high IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "ph" to easily identify it as the private interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAph" for the private high IP address.

Step 9 Click **OK** twice. Then, click **Close**.

Configure Public Ethernet Card

Procedure

Step 1 Right-click **Visible** and select **Properties**.

Step 2 Check **Client for Microsoft Networks**.

Step 3 Check **File and Printer Sharing for Microsoft Networks**.

Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Step 5 Check **Internet Protocol Version 4 (TCP/IPV4)** and click **Properties**.

Step 6 Confirm the **Public IP address**, **Subnet mask**, **Default gateway** and **Preferred DNs server**, and click **Advanced**.

Step 7 On the **Advanced** tab, enter the public IP addresses.

Step 8 On the DNS tab, in the DNS suffix for this connection field, enter the name of the local DNS zone for the server and check **Register this connection's addresses in DNS**.

Step 9 Optional: Add another entry for the public IP address.

Note This IP address should have an entry in the DNS server. This would be required while adding the Router or a Peripheral Gateway through Websetup and PeripheralGatewaySetup respectively.

A host (A) resource record must be created in the **DNS' Forward Lookup Zones**, and can be of the form hostname followed by a suffix "PuH" to easily identify it as the public interface.

For example: If the host name is **RoggerA**, make an entry in the DNS as "RoggerAPuH" for the public IP address.

Step 10 If the server requires access to resources in a different trusting or trusted domain or DNS zone, select **Append these DNS suffixes (in order)** and enter the local DNS zone for the server first, and then add the other secondary zones that represent the trusting or trusted domain.

Step 11 Click **OK** twice. Then, click **Close**.

Set Local Administrator Password

Procedure

Step 1 Open **Computer Management**.

Step 2 In left pane, expand **Local and Users Groups** and select **Users**.

Step 3 In right pane, right-click **administrator** and choose **Set password**.
Displays **Set Password for Administrator** dialog box.

Step 4 Click **Proceed**.

Step 5 Enter **New Password** and **Confirm Password**.

Verify the Machine in Domain

For Unified CCE golden template, the Automation Tool script clones and deploys the virtual machines automatically to the destination domain. Complete the following procedure to verify if the Virtual Machine is placed in destination domain.

For small contact center deployment model Agent PG can be in customer domain instead of service provider domain.

Procedure

Step 1 Log in to the Unified CCE machine.

Step 2 Navigate to **Start** > **All Programs** > **Administrative Tools** > **Server Manager** to verify if the Virtual Machine is mapped to correct domain. If the machine is not in Domain, follow the below steps.

Step 3 Click **Change System Properties** on Right side panel to open System Properties.

Step 4 In Computer name tab, Click **Change**.

Step 5 Choose **Domain** radio button to change the member from Workgroup to Domain.

Step 6 Enter fully qualified Domain name and Click **OK**.

Step 7 In Windows security pop-up, Validate the domain credentials and click **OK**.

Step 8 On successful authentication, Click **OK**.

Step 9 Reboot the server and login with domain credentials.

Configure the Domain Manager

This procedure creates a organizational unit (Cisco_Unified CCE, facility,instance) from any of the Unified CCE PGs.

Note The domain manager is a one-time configuration. You do not need to configure the domain manager for side B.

Note For Small Contact Center agent deployment model, follow the below procedure to create OU structure for the Agent PG in sub customer domain similar to the Unified CCE domain or skip the below procedure if you want to install Agent PG in the Unified CCE domain.

Procedure

Step 1 Click the **Windows Start** icon, and then select the Downward Arrow icon to display all applications.

Step 2 Select the **Domain Manager** icon from the list of applications.

Step 3 Log in as a user who has permissions to create organizational units (OUs) in the domain.

Step 4 In the section on the left, expand the domain.

Step 5 Add the Cisco root as Cisco_Unified CCE :

a) Under the Cisco root, click **Add**.

b) Select the **OUs** under which you want to create the Cisco root OU and click **OK**.

When you return to the **Domain Manager** dialog box, the Cisco root OU appears either at the domain root or under the OU that you selected. You can now add the facility.

Step 6 Add the facility organizational unit (OU):

a) Select the Cisco root OU under which you want to create the Facility OU.

b) In the right section, under **Facility**, click **Add**.

c) Enter the name for the **Facility**and click **OK**.

Step 7 Add the Instance OU:

a) Navigate to and select the Facility OU under which you want to create the Instance OU.

b) In the right section, under , click **Add**.

c) Enter the instance name and click **OK**.

Step 8 Click **Close**.

Configure Unified CCE Encryption Utility

Procedure

Step 1 Start **All Programs** > **Cisco Unified CCE Tools**.

Step 2 Select **SSL Encryption Utility**.

Step 3 Click the **Certificate Administration** tab.

Step 4 Click **Uninstall**. Select **Yes**.

Step 5 When the uninstallation completes, choose **Install**.

You see a stream of messages, ending with *SSL Certificate successfully installed*.

Step 6 Click **Close**.

What to do next

Create and Bind System CLI Certificate, on page 11

Create and Bind System CLI Certificate

Complete the following procedure to create and bind the system CLI certificate:

Procedure

Step 1 Open the command prompt.

Step 2 Enter the command **cd C:\icm\serviceability\diagnostics\bin** and press **Enter**.

Step 3 Enter the command **DiagFwCertMgr /task:CreateAndBindCert** and press **Enter**.

Configure SQL Server for CCE Components

Configure SQL Server on both the Unified CCE Rogger and the Unified CCE AW-HDS-DDS.

Procedure

Step 1 Click the **Windows Start** icon, and then select the Downward Arrow icon to display all applications.

Step 2 Open **Microsoft SQL Server Management Studio**.

Step 3 Log in.

Step 4 Expand **Security** and then **Logins**.

Step 5 If the BUILTIN\Administrators group is not listed:

a) Right-click **Logins** and select **New Login**.

b) Click **Search** and then **Locations** to locate BUILTIN in the domain tree.

c) Type **Administrators** and click **Check Name** and then **OK**.

d) Double-click **BUILTIN\Administrators**.

e) Choose **Server Roles**.
f) Ensure that **public** and **sysadmin** are both checked.

Allocate a Second Virtual Hard Drive

After deploying the OVA files, the second hard drive is no longer automatically created. To create a second hard drive:

Procedure

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

Step 2 In the **Virtual Hardware** tab, click on **Add New Device**.

Step 3 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.

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

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, as calculated by the Database Estimator tool.

Step 4 On the **Disk Provisioning** section, choose **Thick provision Lazy Zeroed**.

Step 5 In the **VM Options** > **Advanced Options** section, retain the default options.

Step 6 Click **OK** to confirm the changes.

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

Configure the Unified CCE Logger

Configure the Unified CCE logger for Side A and Side B.

Note Ensure that your browser is enabled.

Procedure

Step 1 Launch the **Unified CCE Web Setup**.

Step 2 Sign in using as domain user having local Administrator permissions.

Step 3 Click **Instance Management**, and then click **Add**.

Step 4 In the **Add Instance** window, select **Facility and Instance** from the drop-down list.

Step 5 In the **Instance Number** field, enter `0` and click **Save**.

Step 6 Configure the logger database as follows:

a) Open **ICMDBA** application.
b) Select **Server** > **Instance** (logger being installed).
c) Right-click the instance name and choose **Create** to create the logger database.
d) In **Select Component** dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.
e) In **Select Logger Type** window, select **Enterprise** from the drop-down list. Click **OK**.

Step 7 In **Create Database** window, configure the following to create the Log:

a) From **DB Type** drop-down list, choose either **side A** or **side B**.
b) Choose **Region**.
c) In **Storage** pane, click **Add**.

Step 8 In **Add Device** dialog box, configure as follows:

a) Select **Log**.
b) Choose **C** drive.
c) Accept the default in the size field.
d) Click **OK**.

Step 9 In **Create Database** window, in **Storage** section, click **Add**.

Step 10 In **Add Device** dialog box, configure as follows:

a) Select **Data**.
b) Choose the secondary drive (typically E).
c) Accept the default in the size field.
d) Click **OK**.

Step 11 In **Create Database** window, click **Create** and click **Start**.

When you see the successful creation message, click **OK** and click **Close**.

Step 12 Configure the logger component as follows:

a) Return to **Unified CCE Web Setup**. You might need to log in again.
b) Choose **Component Management** > **Loggers**.
c) Click **Add** and choose the **Instance**.
d) From **Fault Tolerance Mode** drop-down list, choose **Duplexed** option and click **Next**.
e) In **Central Controller Connectivity** window, enter the host names for Sides A and B for the Router Private Interface and Logger Private Interface and click **Next**.

Step 13 In **Additional Options** window, configure as follows:

a) Check the **Enable Historical/Detail Data Replication** check box.
b) Check the **Display Database Purge Configuration Steps** check box and click **Next**.

Step 14 In **Data Retention** window, in the data retention table, retain the default values and click **Next**.

Step 15 In **Data Purge** window, configure purge for a time when there is low demand on the system. Click **Next**.

Step 16 In the **Summary** window

a) Enter the domain user.

Verify that the user is created in the specified domain,

For more information on creating the domain user, see Create Users in Active Directory.

b) Enter the valid password.

c) Review the Summary and click **Finish**.

Note Do not start service until all Unified CCE components are installed.

Caution Use the same domain user account for all the distributor and logger services. If you want to use different domain accounts for the logger and the distributor, ensure that the distributor service user account is added to the local logger `UcceService` groups on Side A and Side B.

What to do next

Set database and log file size, see Database and Log File Size, on page 14.

Database and Log File Size

Complete the following procedure to increase the database and log sizes.

Before you begin

To calculate database and log file size, download and use the Database Size Estimator from https://software.cisco.com/download/type.html?mdfid=268439622&catid=null.

Alternative option is to size the database and log using the values from the following table.

Procedure

Step 1 Open **SQL Server Management Studio**.

Step 2 Click **Connect**. In the left pane, expand **Databases**.

Step 3 Right-click Logger database [<Instance>_<Side>] and select Properties..

Step 4 In the left pane, select **Files**. Ensure that **Auto Growth** is disabled for data and enabled for log files. Log files automatically grow in 10 percent increments.

Step 5 Set the initial size of the data and log files according to the Database Size Estimator or from the following table:

Table 2: Data and Log File Size

Database	Data size(MB)	Log Size(MB)	Deployment Type
Side A, Side B	409600	1024	12000 and 24000 agent

Database	Data size(MB)	Log Size(MB)	Deployment Type
Side A, Side B	122900	1024	Other HCS for CC for CC Deployments

Configure the Unified CCE Router

Procedure

Step 1 Launch the Unified CCE Web Setup.

Step 2 Sign in as the domain user with local Administrator permission.

Step 3 Click **Instance Management**, and then click **Add**.

Step 4 In the **Add Instance** window, select **Facility and Instance** from the drop-down list.

Step 5 In the **Instance Number** field, enter `0`. Click **Save** .

Step 6 Select **Component Management** > **Routers**.

Step 7 Click **Add** to set up the Call Router.

Step 8 In the **Deployment window**, select the appropriate **Side**.

Step 9 Select **Duplexed** as Fault Tolerance Mode. Click **Next**.

Step 10 In the **Router Connectivity** window, configure the Private Interface and Public (Visible) Interfaces. Click **Next**.

Step 11 In the **Enable Peripheral Gateways** dialog box, enter the following in the Enable Peripheral Gateways field. Click **Next**.

- For 2000 agents deployments, typically `2-4`.
- For 4000 agents deployment, typically `2-4`.
- For 12000 agents deployment, typically `2-16`.
- For 24000 agents deployment, typically `2-32`.

Step 12 In the **Router Options** window, configure as follows:

a) Check **Enable Database Routing**.
b) Check **Enable Quality of Service (QoS)**. (Applicable to Side A only.)
c) Click **Next**.

Step 13 In **Router Quality of Service** window, click **Next**. (Applicable to Side A only.)

Step 14 In the **Summary** window, make sure that the router summary is correct, then click **Finish**.

Note
- Do not start the service until all Unified CCE components are installed.

What to do next

To enable the **DNWildcard**, select the Registry > HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems > ICM > <instance> >RouterA > Router > CurrentVersion > Configurations > Global, and select the DNWildcardEnabled and set to `1`.

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_11.6.1-Day1_2000.zip or file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Rogger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Rogger on Side A.

Step 5 Select the Unified CCE Rogger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click **Start** and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Rogger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCE Rogger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Rogger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Configure Unified CCE AW-HDS-DDS

This section explains the configuration procedures you must perform for the Unified CCE AW-HDS-DDS for Sides A and B.

Table 3: Configuring Unified CCE AW-HDS-DDS for Side A and Side B

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Validate Network Card, on page 35	
3	Configure Unified CCE Encryption Utility, on page 11	
4	Configure SQL Server for CCE Components, on page 11	
5	Allocate a Second Virtual Hard Drive, on page 12	
6	AW-HDS-DDS, on page 17	
7		
8	Verify Cisco Diagnostic Framework Portico, on page 31	
9	Cisco SNMP Setup, on page 31	
10	Set the HCS for CC Deployment Type, on page 20	

AW-HDS-DDS

- Create Instance, on page 17
- Create HDS Database, on page 18
- Configure AW-HDS-DDS, on page 18
- Database and Log File Size, on page 20
- Set the HCS for CC Deployment Type, on page 20

Create Instance

Procedure

Step 1 Launch Unified CCE Web Setup from the desktop and log in using the Domain Administrator credentials to complete the installation.

Step 2 Click **Instance Management**, and then click **Add**.

Step 3 In the Add Instance window, select **Facility** and **Instance** from the drop-down list.

Step 4 In the Instance Number field, enter **0**. Click **Save**.

Create HDS Database

Procedure

Step 1 Configure the HDS database as follows:
a) Choose **Start > Programs > Cisco Unified CCE Tools > ICMdba**.
b) Navigate to **Server > Instance**.
c) Right-click the instance and choose **Create**.

Step 2 In the Select Component dialog box, choose **Administration & Data Server** from the drop-down list. Click **OK**.

Step 3 At the prompt, *SQL Server is not configured properly. Do you want to configure it now?"* Click **Yes**.

Step 4 On the Configure page, in the **SQL Server Configurations** pane check **Memory (MB)** and **Recovery Interval**. Click **OK**.

Step 5 On the Stop Server page, click **Yes** to stop the services.

Step 6 In the **Select AW Type** dialog box, choose **Enterprise** from drop-down list. Click **OK**.

Step 7 In the **Create Database** dialog box, configure as follows:
a) In the DB Type field, choose **HDS** from drop-down.
b) In the Storage pane, click **Add**.

Step 8 In the Add Device dialog box, configure as follows:
a) Select **Data**.
b) Select the secondary drive (typically **E**).
c) Accept the default in the size field.
d) Click **OK**.

Step 9 In the Create Database dialog box, under Storage, click **Add**.

Step 10 In the Add Device dialog box, configure as follows:
a) Select **Log**.
b) Select the **C** drive.
c) Accept the default in the size field.
d) Click **OK**.

Step 11 In the Create Database dialog box, configure as follows:
a) Click **Create**.
b) Click **Start**.
c) Click **OK**.
d) Click **Close**.

Configure AW-HDS-DDS

Complete the following procedure to install the Cisco Unified CCE Administration Server & Real-time Data Server, Historical Data Server, and Detailed Data Server (AW-HDS-DDS).

Before you begin

Create a domain user if a domain user does not exist already for that service account. For more information on creating the domain user, see *Create Users in Active Directory*.

Procedure

Step 1 Choose **Component Management** > **Administration & Data Servers**.

Step 2 Click **Add**.

Step 3 On the Deployment window, choose the current instance.

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

a) Click **Enterprise**.
b) Click **Small to Medium** Deployment Size.
c) Click **Next**.

Step 5 On the Server Role in a Small to Medium Deployment window, configure as follows:

a) Choose the option **Administrator Server Real-time Data Server**, **Historical Data Server**, and **Detailed Data Server (AW-HDS-DDS)**.
b) Click **Next**.

Step 6 On the Administration & Data Servers Connectivity window, configure as follows:

a) Select **Primary Administration & Data Server**.
b) Enter the hostname of the Secondary AW-HDS-DDS in the *Secondary Administration & Data Server field.
c) Enter the site name in the Primary/Secondary Pair (Site) Name field.

Note Ensure that the site name match with the site name defined under **PG Explorer** > **Agent Peripheral** > **Agent Distribution**.

d) Click **Next**.

Step 7 On the Database and Options window, configure as follows:

a) In the Create Database(s) on Drive field, select **E**.
b) Check **Configure Management Service (CMS) Node**.
c) Check **Internet Script Editor (ISE) Server**.
d) Check **Next**.

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

a) For Router Side A enter the host name/IP address machine where Router A resides.
b) For Router Side B enter the host name/IP address machine where Router B resides.
c) For Logger Side A enter the host name/IP address machine where Logger A resides.
d) For Logger Side B enter the host name/IP address machine where Logger B resides.
e) Enter the **Central Controller Domain Name**.
f) Click **Central Controller Side A Preferred**.
g) Click **Next**.

Step 9 In the **Summary** window

a) Enter the domain user of the service account.

Create a domain user if a domain user does not exist already for that service account. For more information on creating the domain user, see Create Users in Active Directory.

b) Enter the valid password.
c) Review the Summary and click **Finish**.

Note Do not start service until all Unified CCE components are installed.

Caution Use the same domain user account for all the distributor and logger services. If you want to use different domain accounts for the logger and the distributor, ensure that the distributor service user account is added to the local logger `UcceService` groups on Side A and Side B.

Database and Log File Size

Complete the following procedure to increase the database and log sizes.

Before you begin

Use Database Size Estimator to calculate database and log file size.

Alternative option is to size the database and log using the values from Table 4: Data and Log File Size, on page 20.

Procedure

Step 1 Open **Microsoft SQL Server Management Studio**.

Step 2 Expand the Database in Object Explorer.

Step 3 Select **HDS database**. Right-click on the database and select **Properties**.

Step 4 Click **Files** to increase the database and log sizes.

Step 5 Ensure that **Auto Growth** is disabled for data and enabled for log files. Log files automatically grow in 10 percent increments.

Step 6 Set the initial size of the data and log files according to Database Size Estimator or from the following table:

Table 4: Data and Log File Size

Database	Data size (MB)	Log Size
<instance>_hds	409600	1024

Set the HCS for CC Deployment Type

Before you begin

- Ensure that a domain user logging into **CCE Web Administration** is part of the `UcceConfig local` group of all Unified CCE AW DB (real-time distributor) machines.

Procedure

Step 1 Launch **CCE Web Administration**.

Step 2 Login with user credentials.

Step 3 Set the HCS for CC for CC Deployment Type

a) Click **Deployment** under the **System** tab

b) Select the Deployment Type from the drop-down list.

Note For small contact center agent deployment, select Deployment type as **HCS for CC 4000 Agents**

c) Click **Save** and click **Yes** on the warning message.

Step 4 View the Deployment Type.

a) Click **Home** tab to view the deployment type

Step 5 View the System Validation Rules

a) Click **Information** under the **System** Tab

b) Click **System Validation**

Step 6 View the System Configuration Limits

a) Click **Information** under the **System** Tab

b) Click **Capacity Info**

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 all the AW 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 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`.

Configure Unified CCE PG

The following table explains the tasks that you must perform to configure Unified CCE PG on both side A and B.

Table 5: Configure Unified CCE Unified PG on Side A and B

Sequence	Tasks	Done?
1	Configure Network Cards, on page 7	
2	Validate Network Card, on page 35	
3	Configure Unified CCE Encryption Utility, on page 11	
4	Configure CUCM Peripheral Gateway, on page 23	
5	Configure VRU Peripheral Gateway, on page 25	
6	Configure MR Peripheral Gateway, on page 27	
7	Configure CTI Server, on page 29	

Sequence	Tasks	Done?
8	Upgrade Cisco JTAPI Client on PG, on page 30	
9	Verify Cisco Diagnostic Framework Portico, on page 31	
10	Cisco SNMP Setup, on page 31	
11	Start Unified CCE Services, on page 34	

Configure CUCM Peripheral Gateway

Complete the following tasks to configure CUCM peripheral gateways for the PG Server on Side A and then repeat the same procedure for Side B.

- Configure CUCM PG, on page 23
- Prepare to Add PG, on page 24
- Add CUCM PG, on page 24
- Add CUCM PIM, on page 24
- After Creating PIMs, on page 25

Configure CUCM PG

Before you begin

You can lauch the **Configuration Manager** after logging into a windows machine only if you are a domain administrator or part of any one of the following groups:

- `UcceConfig Local` group
- `Local administrator` group

Procedure

Step 1 Open **Configuration Manager > PG Explorer**.

Step 2 Select the option **Enable Agent Reporting for CUCMPG1 Routing Client**.

Step 3 Enter the Primary and Secondary CTI address and port information in the **Unified Communications Manager PG** for the Cisco Unified WIM and EIM feature.

Step 4 In the **Agent Distribution** tab, enter a site name in **Administration and Data Server** field.

Prepare to Add PG

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **ICM Instances** pane, click **Add**.

Step 3 In the **Add Instance** window, select the appropriate **Facility** and **Instance Name** from the drop-down list.

Step 4 In the **Instance Number** field, enter `0`.

Step 5 Click **Save**.

Add CUCM PG

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** pane, click **Add**.

Step 3 From the **ICM/CCE/CCH Component Selection** dialog box, select **Peripheral Gateway**.

Step 4 In the **Peripheral Gateway Properties** dialog box:

a) Check the **Production mode** check box.
b) Check the **Auto start at system startup** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) In the **PG Node Properties ID** pane, from the **ID** drop-down list, select the appropriate PG.
e) Select the appropriate side (**Side A** or **Side B**).
f) In the **Client Type Selection** pane, add **CUCM** to the **Selected types**.
g) Click **Next**.

Add CUCM PIM

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **CUCM**.

Step 3 From the **Available PIMS** list, select **PIM**, then click **OK**.

Step 4 In the **CUCM Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID.

Step 7 In the **Agent Extension Length** field, enter the extension length for this deployment.

Note For the SCC deployment model, agent extension length is 8.

Step 8 In the **CUCM Parameters** pane, configure as follows:

a) In the **Service** field, enter the hostname of appropriate Unified Communications Manager subscriber.
b) In the **User ID** field, enter the user ID.
c) In the **User Password** field, enter the Unified Communication Manager password.
d) In the **Mobile Agent Codec** field, select **G.711U or G.711A or G.729**.
e) Click **OK**.

Step 9 Repeat these steps to configure the remaining PIMs.

Unified Communication Domain Manager sets the default password as "pguser", during Unified Communication Manager Integration.

After Creating PIMs

Procedure

Step 1 In the **Logical Controller ID** field, enter the logical controller ID of the PIM.

Step 2 In the **CTI Wrapup Data Delay** field, enter 0, then click **Next**.

Step 3 In the **Device Management Protocol Properties** window:

a) Select the appropriate side (**Side A** or **Side B**).
b) In the **Side A Properties** panel, select **Call Router**.
c) In the **Side B Properties** panel, select **Call Router**.
d) In the **Usable Bandwidth (kbps)** field, retain the default values.
e) In the **Heartbeat Interval (100ms)** field, enter **4**, then click **Next**.

Step 4 In the **Peripheral Gateway Network interfaces** window, enter **PG Private Interfaces** and **PG Visible (Public) Interfaces**.

Step 5 For Side A only:

a) In the **Private Interfaces** pane, click **QoS**.
b) In the **PG Private Link QoS Settings** pane, check the **Enable QoS** check box, then click **OK**.
c) In the **Visible(Public) Interfaces**, click **QoS**.
d) In the **PG Private Link QoS Settings** pane, check the **Enable QoS** check box, then click **OK**.

Note For 12000, 24000, and SCC deployments, if there are six or more Agents PGs, then QoS must be disabled.

Step 6 In the **Peripheral Gateway Network Interfaces** window, click **Next**.

Step 7 In the **Check setup Information** window, click **Next**.

Step 8 In the **Setup Complete** window, click **Finish**.

Note Do not start Unified CCE /CCNodeManager until all Unified CCE components are installed.

Configure VRU Peripheral Gateway

• Add VRU PG, on page 26

- Add VRU PIM, on page 26
- After Creating PIMs, on page 25

Add VRU PG

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** pane, click **Add**.

Step 3 From the **Component Selection** dialog box, select **Peripheral Gateway**.

Step 4 In the **Peripheral Gateway Properties** dialog box:

a) Check the **Production mode** check box.
b) Check the **Auto start at system startup** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) In the **PG Node Properties ID** pane, from the **ID** drop-down list, select **PG3**.
e) Select the appropriate side (**Side A** or **Side B**).
f) In the **Client Type Selection** pane, add **VRU** to the **Selected types**.
g) Click **Next**.

Add VRU PIM

Caution Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see the *Security 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.

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **VRU**.

Step 3 Select the appropriate PIM from the **Available PIMS** list, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the CVP server name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID of CVP server.

Step 7 In the **VRU Hostname** field, enter the hostname of the CVP server.

Step 8 In the **VRU Connect port** field, enter `5000`.

Step 9 In the **Reconnect interval (sec)** field, enter `10`.

Step 10 In the **Heartbeat interval (sec)** field, enter `5`.

Step 11 From the **DSCP** drop-down list, select **CS3(24)**.

Step 12 Check the **Enable Secured Connection** option to enable secured connection.

This establishes a secured connection between VRU PIM and CVP.

Step 13 Click **OK**.

Step 14 Repeat these steps to configure the remaining PIMs.

Configure MR Peripheral Gateway

- Add Media Routing PG, on page 27
- Add Multichannel PIM to 2000 Agent Deployment, on page 27
- Add Outbound PIM, on page 29
- After Creating PIMs, on page 25

Add Media Routing PG

Configure Media Routing PG, though Multichannel and Outbound are not used. In this case, Media Routing PG remains idle or disabled.

Procedure

Step 1 Open **Peripheral Gateway Setup**.

Step 2 In the **Instance Components** pane, click **Add**.

Step 3 From the **Component Selection** dialog box, select **Peripheral Gateway**.

Step 4 In the **Peripheral Gateway Properties** dialog box:

a) Check the **Production mode** check box.
b) Check the **Auto start at system startup** check box.
c) Check the **Duplexed Peripheral Gateway** check box.
d) In the **PG Node Properties ID** pane, from the **ID** drop-down list, select the appropriate PG.
e) Select the appropriate side (**Side A** or **Side B**).
f) In the **Client Type Selection** pane, add **MediaRouting** to the **Selected types**.
g) Click **Next**.

Add Multichannel PIM to 2000 Agent Deployment

Caution Before performing the step to enable the secured connection between the components, ensure that the security certificate management process is completed.

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **Media Routing**.

Step 3 From the **Available PIMS** list, select **MR PIM1**, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID of the Unified CCE component you are adding. The following are the names by which the Unified CCE components are represented in the database. Refer *Peripheral Gateway* page in CCE Admin to get the peripheral ID of the corresponding PIM.

- Name of Outbound is *Outbound*
- Name of ECE is *Multichannel*
- Name of CCP is *Multichannel2*
- Name of THIRD_PARTY_MULTICHANNEL is *MutliChannel3*
- Name of Digital Routing is *DigitalRouting*

Example:

If you are adding ECE, find the component of the name *Multichannel* in the database. Enter the logical controller ID of that component in the **Peripheral ID** field.

Step 7 In the **Application Hostname (1)** field, enter the hostname or the IP address of the ECE services server.

Step 8 In the **Application connection port (1)** field, enter the port number.

Note Use the port number that is on the ECE services server that PIM uses to communicate with the application. The default port is 38001.

Step 9 In the **Application Hostname (2)** field, leave the field blank.

Step 10 In the **Application connection port (2)** field, leave the field blank.

Step 11 In the **Heartbeat interval (sec)** field, enter `5`.

Step 12 In the **Reconnect interval (sec)** field, enter `10`.

Step 13 Check the **Enable Secured Connection** option.

This establishes a secured connection between the MR PIM and the application server.

Ensure that you provide the correct information in the application hostname(1) and Application Connection Port(1) fields.

Step 14 Click **OK**.

Add Outbound PIM

Caution Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see the *Security 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.

Procedure

Step 1 In the **Peripheral Gateway Component Properties** window, click **Add**.

Step 2 From the **Client Type** drop-down list, select **Media Routing**.

Step 3 From the **Available PIMS** list, select **MR PIM2**, then click **OK**.

Step 4 In the **Configuration** dialog box, check the **Enabled** check box.

Step 5 In the **Peripheral name** field, enter the peripheral name.

Step 6 In the **Peripheral ID** field, enter the logical controller ID.

Step 7 In the **Application Hostname (1)** field, enter the hostname or the IP address of Agent PG machine of Side A.

Step 8 In the **Application connection port (1)** field, retain the default value.

Step 9 In the **Application Hostname (2)** field, enter the hostname or the IP address of Agent PG machine of Side B.

Step 10 In the **Application connection port (2)** field, retain the default value.

Step 11 In the **Heartbeat interval (sec)** field, enter `5`.

Step 12 In the **Reconnect interval (sec)** field, enter `10`.

Step 13 Check the **Enable Secured Connection** option.

This establishes a secured connection between MR PIM and Application Server.

Ensure that you provide the correct information in the Application Hostname(1) and Application Connection Port(1) fields.

Step 14 Click **OK**.

Configure CTI Server

Complete the following procedure to configure the CTI server for Side A and Side B.

Caution Before enabling secured connection between the components, ensure that the security certificate management process is completed. For more information on security certificate management, see *Security 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.

Procedure

Step 1 Select **Start > All Programs > Cisco Unified CCE Tools > Peripheral Gateway Setup**.

Step 2 In the Instance Components pane of the Components Setup dialog box click **Add**.

Step 3 In the Component Selection dialog box, click **CTI Server**.

a) Check **Production mode**.
b) Check **Auto start at system startup**.
c) Check **Duplexed CTI Server**.
d) Choose **CG1** for Agent PG1 and choose **CG2** for Agent PG2.
e) Enter the system ID number corresponding to the Agent PG.
For example: Enter 1 for Agent PG1 and 2 for Agent PG2.
f) Click the appropriate side (Side A or Side B).
g) Click **Next**.

Step 4 In the Server Component Properties dialog box, configure as follows:

a) To enable secured connection, check the **Enable Secure-Only Mode** checkbox.
b) Enter the appropriate port number in the Client Connection Port Number field. The default port is 42027 for non-secured connection and 42030 for secured connection. Ensure that the CTI server port matches with the CTI Gateway (CG) configuration.

Step 5 Click **Next**.

Step 6 In the Network Interface Properties dialog box, enter the private interfaces.

Step 7 Enter the public (visible) interfaces and the CG visible interfaces, and click **Next**.

Step 8 Under the Check Setup Information page, verify all the settings, and click **Next**.

Step 9 In the Setup Completed dialog box, click **Finish**.

Step 10 Click **Exit Setup**.

Note Do not start Unified CCE /CC Node Manager until all Unified CCE components are installed.

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 63 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.

Verify Cisco Diagnostic Framework Portico

Do this for the Unified CCE machines.

Procedure

Step 1 Open the command prompt and enter **cd C:**.

Step 2 Enter **cd icm\serviceability\diagnostics\bin** and press **Enter**.

Step 3 Enter **DiagFwCertMgr /task:CreateAndBindCert /port:7890** and press **Enter**.

Step 4 Go to **Start -> Run** and enter **services.msc** to open the Services tool. Make sure the Cisco Diagnostic Framework service is running. If it is not running start it.

Step 5 Open Diagnostic Framework Portico: **Start** > **Programs** > **Cisco Unified CCE Tools** > **Diagnostic Framework Portico**. Then make sure you can log in to the Diagnostic Framework Portico using domain user credentials.

Cisco SNMP Setup

Complete the following procedures to configure Cisco SNMP:

- Add Cisco SNMP Agent Management Snap-In, on page 31
- Save Cisco SNMP Agent Management Snap-In View, on page 32
- Set Up Community Names for SNMP V1 and V2c , on page 32
- Set Up SNMP User Names for SNMP V3 , on page 32
- Set Up SNMP Trap Destinations , on page 33
- Set Up SNMP Syslog Destinations , on page 33

Add Cisco SNMP Agent Management Snap-In

You can configure Cisco SNMP Agent Management settings using a Windows Management Console snap-in.

Complete the following procedure to add the snap-in and change Cisco SNMP Management settings.

Procedure

Step 1 From the Start menu, enter **mmc.exe /32**.

Step 2 From the Console, choose **File** > **Add or Remove Snap-ins**.

Step 3 In the Add or Remove Snap-ins dialog box, choose **Cisco SNMP Agent Management** from the list of available snap-ins. Click **Add**.

Step 4 In the Selected snap-ins pane, double-click **Cisco SNMP Agent Management**.

Step 5 In the Extentions for Cisco SNMP Agent Management dialog box, select **Always enable all available extentions**. Click **OK**.

Step 6 In the Add/Remove Snap-in window, click **OK**. The Cisco SNMP Agent Management Snap-in is now loaded into the console.

Save Cisco SNMP Agent Management Snap-In View

After you load the Cisco SNMP Agent Management MMC snap-in, you can save the console view to a file with a .MSC file extension. You can launch the file directly from Administrative Tools.

Complete the following procedure to save the Cisco SNMP Agent Management snap-in view.

Procedure

Step 1 Choose **File** > **Save**.

Step 2 In the Filename field, enter **Cisco SNMP Agent Management**.

Step 3 In the Save As type field, choose a file name to map to the administrative tools such as **Microsoft Management Console Files(*.msc)**.

Step 4 Click **Save**.

Set Up Community Names for SNMP V1 and V2c

If you use SNMP v1 or v2c you must configure a community name so that Network Management Systems (NMSs) can access the data your server provides. Use SNMP community names to authenticate data exchange of SNMP information. An NMS can exchange SNMP information only with servers that use the same community name.

Complete the following procedure to configure the community name for SNMP v1 and v2c.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 31 and Save Cisco SNMP Agent Management Snap-In View, on page 32.

Procedure

Step 1 Choose **Start** > **All Programs** > **Administrative tools** > **Cisco SNMP Agent Management**.

Step 2 Right-click **Cisco SNMP Agent Management** and choose **Run as administrator**.

Step 3 The Cisco SNMP Agent Management screen lists some of the configurations that require SNMP for traps and system logs.

Step 4 Right-click **Community Names (SNMP v1/v2c)** and choose **Properties**.

Step 5 In the Community Names (SNMP v1/v2c) Properties dialog box, click **Add New Community**.

Step 6 In the Community Name field, enter a community name.

Step 7 In the Host Address List, enter the host IP address.

Step 8 Click **Apply** and click **OK**.

Set Up SNMP User Names for SNMP V3

If you use SNMP v3 you must configure a user name so that NMSs can access the data your server provides.

Complete the following procedure to configure a user name for SNMP v3.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 31 and Save Cisco SNMP Agent Management Snap-In View, on page 32.

Procedure

Step 1 From the Console Root, choose **Cisco SNMP Agent Management** > **User Names (SNMP v3)** > **Properties**.

Step 2 Click **Add New User**.

Step 3 In the User Name field, enter a username.

Step 4 Click **Save**.

Step 5 The username appears in the Configured Users pane at the top of the dialog box.

Step 6 Click **Apply** and click **OK**.

Set Up SNMP Trap Destinations

You can configure SNMP Trap Destinations for SNMP v1, SNMP v2c, and SNMP v3. A Trap is a notification that the SNMP agent uses to inform the NMS of a certain event.

Complete the following procedure to configure the trap destinations.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 31 and Save Cisco SNMP Agent Management Snap-In View, on page 32.

Procedure

Step 1 From the Console Root, choose **Cisco SNMP Agent Management** > **Trap Destinations** > **Properties**.

Step 2 Click **Add Trap Entity**.

Step 3 Click the SNMP version that your NMS uses.

Step 4 In the Trap Entity Name field, enter a name for the trap entity.

Step 5 Choose the User Name/Community Name that you want to associate with this trap. This list is auto-populated with existing configured users/community names.

Step 6 Enter one or more IP addresses in the IP Address entry field. Click **Insert** to define the destinations for the traps.

Step 7 Click **Apply** and click **Save** to save the new trap destination.

The trap entity name appears in the Trap Entities section at the top of the dialog box.

Step 8 Click **OK**.

Set Up SNMP Syslog Destinations

You can configure Syslog destinations for SNMP from the Cisco SNMP Agent Management Snap-in.

Complete the following procedure to configure Syslog destinations.

Procedure

Step 1 From the Console Root, choose **Cisco SNMP Agent Management** > **Syslog Destinations** > **Properties**.
Step 2 Choose an Instance from the list box.
Step 3 Check **Enable Feed**.
Step 4 Enter an IP address or host name in the Collector Address field.
Step 5 Click **Save**.
Step 6 Click **OK** and restart the logger.

Start Unified CCE Services

The Unified CCE components run as a Windows service on the host computer. You can start, stop, or cycle these services from the **Unified CCE Service Control tool** on the desktop.

Note This procedure is required for activating Unified CCE services. However, you must postpone this task until you install Unified CCE components in all virtual machines given in the deployment model.

Procedure

Step 1 On eachUnified CCE Server machine, open **Unified CCE Service Control**.
Step 2 Start the **Unified CCE component** services.

Configure Unified CVP

This section explains the procedures to configure Unified CVP.

Sequence	Task	Done?
1	Configure Unified CVP Server, on page 34	
2	Configure Unified CVP Reporting Server, on page 38	
3	Configure Cisco Unified CVP Operations Console, on page 43	

Configure Unified CVP Server

This section explains the procedures to configure Unified CVP Server.

Sequence	Task	Done?
1	Validate Network Card, on page 35	
2	Setup Unified CVP Media Server IIS, on page 35	
3	Setup FTP Server, on page 36	

Validate Network Card

Procedure

Step 1 Select **Start** and right-click **Network.**

Step 2 Select **Properties**. Then select **Change Adapter Settings**.

Step 3 Right-click **Local Area Connection** and select **Properties.**

Step 4 Uncheck **Internet Protocol Version 6 (TCP/IPV6)**.

Step 5 Check **Internet Protocol Version 4** and select **Properties**.

Step 6 Confirm the data for Visible IP addresses, Subnet mask, Default gateway and Preferred and alternate DNS servers.

Step 7 Click **OK**.

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 4.5
  - ASP.NET 4.5
  - 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**.

Setup FTP Server

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 Goto **Start** > **Administrative Tools**.

Step 2 Choose **Sever Manager** and click **IIS**.

Step 3 Right-click on the server that you want to enable FTP server and choose **Internet Information Services (IIS) Manager** option from submenu.

Step 4 Goto **Connections** panel:

a) Expand CVP server that you want to add FTP site.
b) Right-click on **Site** and choose **Add FTP Site** option from submenu.

Step 5 Enter **FTP Site Name**.

Step 6 Browse `C:\Inetpub\wwwroot` in **Physical Path** field and click **Next**.

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

Step 8 Enter **Port** number.

Step 9 Check **No SSL** check box and click **Next**.

Step 10 Check **Anonymus** and **Basic** check boxes in **Authentication** panel.

Step 11 Choose **All Users** from **Allow Access To** drop-down list.

Step 12 Check **Read** and **Write** check boxes and click **Finish**.

Configure Basic Settings for FTP Server

Procedure

Step 1 Navigate to **FTP server** that you have created in **Connections** tab.

Step 2 Goto **Actions** tab and click **Basic Settings**.

Step 3 Click **Connect As**.

Step 4 Choose **Application User (pass-through authentication)** option and click **OK**.

Step 5 Click **OK** in **Edit Site** window.

Configure Unified CVP Reporting Server

Note

- There is one Unified CVP Reporting Server for 2000 agent deployment.
- There are two Unified CVP Reporting Servers for other agent deployments.

This table lists the procedures to configure Unified CVP reporting server.

Sequence	Task	Done ?
1	Validate Network Card, on page 35	?
2	Allocate a Second Virtual Hard Drive, on page 12	?
3	Unified CVP Reporting Users, on page 38	?
4	Create Data Source for Cisco Unified CVP Report Data, on page 40	?

Unified CVP Reporting Users

Create Reporting Users

Who can create a user:

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

Unified CVP reporting users can sign in to Unified Intelligence Center only if they exist in the Administration console as Superusers or if Active Directory (AD) is configured in the Unified Intelligence Center Administration console for their domain:

- Superusers who are added are considered to be IP Multimedia Subsystem (IMS) users.
- Users who are authenticated through Active Directory are considered to be Lightweight Directory Access Protocol (LDAP) users.

Both IMS users and LDAP users can log in to Unified Intelligence Center reporting and are restricted to the limited Login User role until the Unified Intelligence Center reporting security administrator gives them additional roles and flags them as active users.

Create Superusers

Procedure

Step 1 Log in to the Cisco Unified Intelligence Center Administration Console `(https://<HOST ADDRESS>/oamp)`.

Step 2 Navigate to **Admin User Management > Admin User Management** to open the Users page.

Step 3 Click **Add New** to add and configure a new user or click an existing username to edit the configuration for that user.

This page has three tabs: General, Credentials, and Policy. For information about completing these tabs, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/en/US/products/ps9755/prod_maintenance_guides_list.html or the Administration console online help.

Step 4 Click **Save**.

Set Up Active Directory Server for LDAP Users

Configure the Active Directory tab in the Cisco Unified Intelligence Center Administration console so that Unified CVP reporting users can log in to the Unified Intelligence Center reporting application with the user name and password that is defined in their domain.

Procedure

Step 1 In the Cisco Unified Intelligence Center Administration application, navigate to **Cluster Configuration** > **Reporting Configuration** and select the Active Directory tab.

Step 2 Complete all fields on this page, referring to the online help for guidance.

Step 3 Click **Test Connection**.

Step 4 When the connection is confirmed, click **Save**.

Sign In to Cisco Unified Intelligence Center Reporting Interface

Who can sign in to the Unified Intelligence Center reporting interface:

- Initially, the System Application User who is the default Superuser.
- Eventually, any Unified CVP user who was created in the Administration Console as an IMS superuser or an LDAP user.

Perform the following procedure to sign in to the Unified Intelligence Center reporting interface.

Procedure

Step 1 Sign in to the Cisco Unified Intelligence Center Administration Console (*https://<HOST ADDRESS>/oamp*).

Step 2 Navigate to **Control Center** > **Device Control**.

Step 3 Click on the name of the Member node you want to access. This opens the Cisco Unified Intelligence Center login page for that member.

Step 4 Enter your user ID and password. The Overview page appears.

Step 5

What to do next

If you have CVP Reporting as an on-box VM or an external server, refer to sections in the Configure Unified Intelligence Center section for information on creating the data source for Unified CVP and importing CVP report templates.

Create Report Template

Follow these steps to create a Unified CVP Report Template from the Unified Intelligence Center at *https://<hostname of CUICPublisher>:8444/cuic*.

Sequence	Task	Done?
1	Create Data Source for Cisco Unified CVP Report Data, on page 40	
2	Obtain Cisco Unified CVP Report Templates , on page 41	
3	Import Reports, on page 41	

Create Data Source for Cisco Unified CVP Report Data

You can create or edit a data source only if you are assigned with a System Configuration Administrator role.

To create a data source, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Configure** > **Data Sources**.

Step 2 In the **Data Sources** window, click **New**.

Step 3 In the **Create Data Source** dialog box, enter the datasource **Name**, **Description**, and select the **Data Source Type**.

Step 4 Click **Next**.

Step 5 In the data source details page, enter the following (Primary Node tab):

Field	Description
Host Settings	
Datasource Host	The hostname or IP address of the target data source.
Port	The port number that allows Unified Intelligence Center to communicate with the database. **Note** The port number is a mandatory field only for the Informix database.
Database Name	Enter the name of the database.
Instance	Enter the instance of the database. **Note** The name of the database instance is a required field only for Informix databases.
Time zone	Select the time zone that the database is located in.
Authentication Settings	
Database User ID	The user ID required to access the database.
Password	The password for the user ID required to access the database.

Field	Description
Charset	The character set that is used by the database.
Max Pool Size	The maximum pool size. **Note** Value ranges from 5 to 200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs.

Step 6 Click **Test Connection** to ensure that the database is accessible and the credentials provided are correct.

Step 7 Click the **Secondary Node** tab to configure a failover for the data source.

Step 8 Check the **Enable Failover** check box to configure a failover for the data source.

Step 9 Enter the required details for the failover data source. (Refer step 5)

Step 10 Click **Save**.

Obtain Cisco Unified CVP Report Templates

Who can obtain import Unified CVP report templates: any user in your organization.

The Unified CVP reporting template XML files are installed with Unified CVP. Locate them and copy them to a Cisco Unified Intelligence Center client workstation.

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

Procedure

Step 1 In the Unified CVP server, locate the Unified CVP template files. These are XML files that reside on the reporting server in %CVP_HOME%\CVP_Reporting_Templates. You can also find them in the Installation directory \Downloads and Samples\Reporting Templates.

Step 2 Choose the files and copy them to the client computer from where you can launch the Unified Intelligence Center Reporting web application.

Import Reports

You can import the Unified Intelligence Center report, which is in either .xml or .zip file format.

The imported report retrieves data for the following entities:

- Report
- Report Definition
- Value Lists
- Views
- Thresholds
- Drilldowns
- Template Help

Note Each report template help folder has a size limit of 3 MB. If the folder size exceeds this limit, the system does not load the help content.

Note You cannot import Report Filters and Collections.

Ensure that the data source is used to import the Report Definition is configured in Unified Intelligence Center. Also, ensure that data source is used by any value list that is defined in Unified Intelligence Center, if the report definition has any value list defined.

To import reports, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Reports**.

Step 2 In the **Reports** listing page, click **Import**.

Step 3 Click **Browse** to select the file (.xml or .zip format) to be imported.

Note Maximum file size for .zip file format is 60 MB and for .xml file format is 3 MB.

Step 4 Select the required file and click **Open**.

Step 5 Select the file location from the **Save to Folder** list to save the file.

Step 6 Click **Upload**.
Once the file is successfully uploaded, the table gets populated with the corresponding report template, current available version, and incoming version of the files being imported.

Step 7 Select a Data Source for the Report Definition only if the Report Definition for the report being imported is not defined in Unified Intelligence Center.

Step 8 Select a Data Source for the Value List that is defined in the Report Definition.

Note Selection of a Data Source for the Value List is mandatory:

- If the Value List does not use the same Data Source as the Report Definition.
- For Real Time Streaming Report Definitions.

Step 9 Select the files to import or overwrite.

- Overwrite—If the report being imported exists in the Unified Intelligence Center.
- Import—If the report being imported is the new set of report files.

Step 10 Click **Import**.

Note

- Importing a report to a different version of Unified Intelligence Center is not supported. However, when you upgrade Unified Intelligence Center, report templates continue to work in the upgraded version.
- Importing manually edited XMLs is not supported.

Configure Cisco Unified CVP Operations Console

Sequence	Task	Done?
1	Validate Network Card, on page 35	
2	Enable Unified CVP Operations Console, on page 43	
3	Configure Unified CVP Call Server Component, on page 44	
4	Configure Unified CVP Server Component, on page 45	
5	Configure Unified CVP Reporting Server, on page 45	
6	Configure Unified CVP Media Server, on page 46	
7	Install Unified CVP licenses, on page 46	
8	Configure Gateways, on page 47	
9	Add Unified CCE Devices, on page 48	
10	Add Unified Communications Manager Devices, on page 48	
11	Add Unified Intelligence Center Devices , on page 49	
12	Transfer Scripts and Media Files, on page 47	
13	Configure SNMP, on page 47	
14	Configure SIP Server Group, on page 49	
15	Configure Dialed Number Patterns, on page 50	

Enable Unified CVP Operations Console

Complete the following procedure on the Unified CVP OAMP server to enable the Unified CVP Operations Console.

Procedure

Step 1 Go to **Start > Run** and type **services.msc**.

Step 2 Check that Cisco CVP OPSConsoleServer service is running. If it is not, right-click that service and click **Start**.

Step 3 Go to **Start > All Programs > Cisco Unified Customer Voice Portal > Operation Console** to open the Unified CVP OPSConsole page. If you are using Microsoft Internet Explorer, you will need to accept the self-signed certificate.

Configure Unified CVP Call Server Component

Note

- There is one Unified CVP server on Side A and one Unified CVP server on side B for the 500 agent deployment.
- There are two Unified CVP servers on Side A and two Unified CVP server on side B for the 1000 agent deployment.
- There are eight Unified CVP servers on Side A and eight Unified CVP server on side B for the 4000 agent deployment.

Procedure

Step 1 On the Unified CVP OAMP server, go to **Start** > **All Programs** > **Cisco Unified Customer Voice Portal**.

Step 2 Click **Operations Console** and log in.

Step 3 Navigate to **Device Management > Unified CVP Call Server**.

Step 4 Click **Add New**.

Step 5 On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server. Check **ICM**, **IVR**, and **SIP**. Click **Next**.

Step 6 Click the **ICM** tab. For each of the Cisco Unified CVP Call Servers, retain the default port of 5000 for the VRU Connection Port.

Step 7 Click the **SIP** tab:

a) In the Enable outbound proxy field, select **No**.
b) In the Use DNS SRV type query field, select **Yes**.
c) Check **Resolve SRV records locally**.

Step 8 Click the **Device Pool** tab. Make sure the default device pool is selected.

Step 9 (Optional) Click the **Infrastructure** tab. In the Configuration Syslog Settings pane, configure these fields as follows:

a) Enter the IP address or the hostname of the syslog server.

Example:

Prime server

b) Enter **514** for the port number of the syslog server.
c) Enter the name of the backup server to which the reporting server writes log messages.
d) In the Backup server port number field, enter the port number of the backup syslog server.

Step 10 Click **Save & Deploy**.

Step 11 Repeat this procedure for the remaining Unified CVP Servers.

Configure Unified CVP Server Component

Complete the following procedure to configure the VXML Server component for the Cisco Unified CVP Servers.

Procedure

Step 1 In the Unified CVP Operations console, navigate to **Device Management** > **Unified CVP VXML Server**.

Step 2 Click **Add New**.

Step 3 On the General tab, enter the IP address and the hostname of the Cisco Unified CVP Server.

Step 4 Configure the primary and backup CVP Call Servers.

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

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

Step 7 Click **Save & Deploy**.

Step 8 Repeat this procedure for all CVP Servers.

Configure Unified CVP Reporting Server

Complete the following procedure to configure the Unified CVP Reporting Server component in the Operations Console.

Note To load balance to the CVP reporting server, there are 2 CVP reporting servers deployed, one on each side. When a customer has 2 reporting servers, the customer should configure CVP Reporting server Side A and associate all the side A CVP call servers, and for Side B reporting server, associate all the CVP call servers belongs to side B, this is because each CVP call server and each VXML server can be associated with only one reporting server. Be aware that the reports cannot span multiple Informix databases. Side A call servers reports only of side A reporting server and side B call servers reports only of side B reporting server.

If the customer chooses to have a single CVP reporting server, the customer should associate all the call servers to the single reporting server. During temporary database outages, messages are buffered to file and are inserted into the database after the database comes back on line. The amount of time that messages can be buffered depends on the system.

Procedure

Step 1 In the CVP Operations Console, navigate to **Device Management** > **Unified CVP Reporting Server**.

Step 2 Click **Add New**.

Step 3 On the **General** tab, configure the following:

a) Enter the IP address.

b) Enter the hostname.

c) Select all associated Unified CVP Call Servers Available.

Step 4 Configure the following on the **Infrastructure** tab:

a) Accept the default Maximum Threads, Statistics Aggregation Interval, and Log File Properties settings.
b) Enter the IP address or the hostname of the Syslog server to which the reporting server sends syslog events.

Example:

Prime server

c) Enter **514** for the Syslog server port number.
d) Enter the IP address or the hostname of the optional Backup server to which the reporting server sends syslog events.
e) Enter the optional Backup server port number.

Step 5 Click **Save & Deploy**.

Step 6 Repeat Steps 1 through 5 for all CVP Reporting Servers.

Configure Unified CVP Media Server

Procedure

Step 1 In the CVP Operations Console, navigate to **Device Management > Media Server**.

Step 2 Click **Add New**.

Step 3 On the **General** tab, configure the following.

a) Enter the IP address and the hostname of the Unified CVP server.
b) Check **FTP Enabled**.
c) Either Check **Anonymous Access** or enter the credentials.
d) Click **Test SignIn** to validate the FTP access.

Step 4 Click **Save**.

Step 5 Repeat Step 1 through 4 for all Media Servers.

Step 6 After you configure all Media Servers, click **Deploy**.

Step 7 Click **Deployment Status** to make sure that you applied the configuration.

Step 8 In the CVP Operations Console, navigate to **Device Management > Media Server**.

Step 9 Change Default Media Server from **None** to any one of the Unified CVP servers. Then click **Set**.

Step 10 Click **Deploy**.

Install Unified CVP licenses

Procedure

Step 1 Sign in to the **CVP Operations Console**.

Step 2 Choose **Bulk Administration** > **File Transfer** > **Licenses**.

Step 3 In the Select device type field, choose **All Unified CVP devices**.

Step 4 Browse and select the license file.

Step 5 Click **Transfer**.

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

Configure Gateways

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **Device Management** > **Gateway**.

Step 2 Click **Add New**.

Step 3 On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the hostname.
c) Choose the Device Type.
d) In the Username and Passwords pane, enter the username, password, and enable password.

Step 4 Click **Test Sign-in** to verify that a connection with the gateway can be established and that the credentials are correct.

Step 5 Click **Save**.

Step 6 Repeat for every gateway.

Transfer Scripts and Media Files

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

Procedure

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

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

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

Step 4 Click **Default Gateway files**.

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

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

Configure SNMP

Procedure

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

Step 2 Click **Add New**.

a) On the **General** tab, name the community string.
b) On the **Devices** tab, select the required device from the list of available devices.
c) Click **Save and Deploy**.

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

a) Navigate to **SNMP** > **V1/V2c** > **Notification Destination**.
b) Click **Add New**.
c) Complete the fields.
d) Select the **Devices** tab and assign the SNMP notification destination to a device.
e) Click **Save and Deploy**.

Add Unified CCE Devices

Procedure

Step 1 Log in to the **Unified CVP Operations Console**.
Step 2 Choose **Device Management** > **Unified ICM**.
Step 3 Click **Add New**.
Step 4 On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Serviceability.
d) Enter the Username.
e) Enter the Password.
f) Confirm Password.
g) Accept the default port.

Step 5 Click **Save**.
Step 6 Repeat Steps 1 to 5 for all Unified CCE machines.

Add Unified Communications Manager Devices

Procedure

Step 1 Log in to the **CVP Operations Console**.
Step 2 Choose **Device Management** > **Unified CM**.
Step 3 Click **Add New**.
Step 4 On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Synchronization.
d) Enter the Username.

e) Enter the Password.
f) Confirm Password.
g) Accept the default port.

Note For Small contact center deployment add the NAT IP address of the unified CM.

Step 5 Click **Save**.

Step 6 Repeat Steps 1 to 5 for all Unified Communications Manager Devices.

Add Unified Intelligence Center Devices

Procedure

Step 1 Log in to the **CVP Operations Console**.

Step 2 Navigate to the Cisco Unified Intelligence Center Device. Choose **Device Management** > **Unified IC**.

Step 3 Click **Add New**.

Step 4 On the General tab, configure as follows:

a) Enter the IP address.
b) Enter the Hostname.
c) Check Enable Serviceability.
d) Enter the Username.
e) Enter the Password.
f) Confirm Password.
g) Accept the default port.
h) Associate all the existing CVP Reporting Servers.

Step 5 Click **Save**.

Configure SIP Server Group

SIP Server Groups are required for Cisco Unified Communications Manager and Gateways.

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **System** > **SIP Server Group** .

Step 2 Create a server group for the Cisco Unified Communications Manager devices:

a) On the General tab, click **Add New**.
b) Fill in the **SRV Domain Name FQDN** field with a value that will also be used in the Cluster FQDN setting in Enterprise Parameters in Communications Manager. For example, cucm.cisco.com.
c) In the **IP Address/Hostname** field, enter an IP address or hostname for the Unified Communications Manager node.
d) Click **Add**.
e) Repeat Steps c and d for each Unified Communications Manager subscriber. Click **Save**.

Note Do not put the Publisher node in the server group.

SIP server group for Communications Manager is not required for SCC deployment as there is no direct SIP trunk created from Communications Manager to CVP in SCC model.

Step 3 Create a server group for the gateway devices:

a) On the General tab, click **Add New**.
b) In the **SRV Domain Name FQDN** field, enter the SRV Domain Name FQDN. For example vxmlgw.cisco.com.
c) In the **IP Address/Hostname** field, enter an IP address or hostname for each gateway.
d) Click **Add**.
e) Repeat Steps c and d for each gateway. Click **Save**.

Add all VXML gateways as appropriate for deployment and branches. Adding all VXML gateways to the server group will load balance calls across all the member server group gateways.

Step 4 Associate these server groups to all Unified CVP Call Servers:

a) On the **Call Server Deployment** tab, move all Unified CVP Call Servers from the **Available** list to the **Selected** list.
b) Click **Save and Deploy**.

Note In the small contact center agent deployment, CUBE(SP) does not support FQDN configuration, therefore, you cannot create SIP server group pointing to CUBE(SP) for each sub customer.

Note
- In the small contact center agent deployment, CUBE(SP) does not support FQDN configuration, therefore, you cannot create SIP server group pointing to CUBE(SP) for each sub customer.
- In 12000 and 24000 agent deployment model, each CUCM cluster should have one SIP Server group with their subscriber nodes.

Configure Dialed Number Patterns

Dialed number patterns are required for:

- Agent Device
- Network VRU
- Ringtone
- Error

Procedure

Step 1 In the Unified CVP Operations Console, navigate to **System** > **Dialed Number Pattern**.

Step 2 For each dialed number pattern in the following table:

a) Click **Add New**.
b) In the **Dialed Number Pattern** field, enter the dialed number pattern.

c) In the **Description** field, enter a description for the dialed number pattern.
d) In the **Dialed Number Pattern Types** pane, check the specified dialed number pattern types.
e) Click **Save**.

Step 3 After you configure all dialed number patterns, click **Deploy**.

Step 4 Click **Deployment Status** to make sure that you applied the configuration.

Dialed number pattern	Description	Dialed number pattern types
91*	Ringtone	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com). Check **Enable Send Calls to Originator**.
92*	Error	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example, vxmlgw.cisco.com). Check **Enable Send Calls to Originator**.
The agent extension pattern. For example, enter 500* where the range of agent extensions is 5001 to 500999.	Agent Device.	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both the Unified Communications Manager gateway. Check **Enable RNA Timeout for Outbound Calls**. The default timeout value is 60 seconds.
777*	Network VRU Label	Check **Enable Local Static Route**. Route to SIP Server Group and IP Address/Hostname/Server Group Name are both VXML Gateway (for example vxmlgw.cisco.com). Check **Enable Send Calls to Originator**.
The agent extension pattern for the sub customer in SCC model. For example, enter 500* where the range agent extensions is 5001 to 500999.	Agent Device Label for the sub customer in the SCC model.	Check Enable Local Static Route. In IP Address/Hostname/Server Group field provide the signaling IP address and port of the CVP adjacency in CUBE(SP) in the format:< IP Address>:<Port number> For each sub customer a unique port must be configured. Check Enable RNA Timeout for Outbound Calls. The timeout is 15 seconds.

Note In 12000 and 24000 agent deployment model, each CUCM cluster should have separate Dialed number Pattern with their agent extension range.

Configure Cisco IOS Enterprise Voice Gateway

Complete the following procedure to configure the Cisco IOS Voice Gateway. Instructions are applicable to both TDM and Cisco UBE Voice gateways, unless otherwise noted.

Note Complete all configuration steps in **enable** > **configuration terminal** mode.

```
logging buffered 2000000 debugging
no logging console
service timestamps debug datetime msec localtime
ip routing
ip cef
ip source-route
interface GigabitEthernet0/0
     ip route-cache same-interface
     duplex auto
     speed auto
     no keepalive
     no cdp enable

voice service voip
     no ip address trusted authenticate
     ip address trusted list
          ipv4 0.0.0.0 0.0.0.0 # OR an explicit Source IP Address Trust List
     allow-connections sip to sip
     signaling forward unconditional
```

Configure Ingress Gateway

Procedure

Step 1 Configure global settings.

```
voice service voip
 no ip address trusted authenticate
 allow-connections sip to sip
 signaling forward unconditional
 # If this gateway is being licensed as a Cisco UBE the following lines are also required
 mode border-element
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0              # Or an explicit Source IP Address Trust List
sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

Step 2 Configure voice codec preference:

```
voice class codec 1
     codec preference 1 g711ulaw
     codec preference 2 g729r8
```

Step 3 Configure default services:

```
#Default Services
application
     service survivability flash:survivability.tcl
```

Step 4 Configure gateway and sip-ua timers:

```
gateway
 media-inactivity-criteria all
 timer receive-rtp 1200

sip-ua
 retry invite 2
 retry bye 1
 timers expires 60000
 timers connect 1000
 reason-header override
```

Step 5 Configure POTS dial-peers:

```
# Configure Unified CVP survivability
dial-peer voice 1 pots
     description CVP TDM dial-peer
     service survivability
     incoming called-number .T
     direct-inward-dial
```

Step 6 Configure the switch leg:

```
#Configure the Switch leg where
# preference is used to distinguish between sides.
# max-conn is used prevent overloading of Unifed CVP
# options-keepalive is used to handle failover
# Note: the example below is for gateways located on the A-side of a geographically
#distributed deployment
# Note: Ensure that you configure switch dial-peers for each Unified CVP server.

dial-peer voice 70021 voip
     description Used for Switch leg SIP Direct
     preference 1
     max-conn 225
     destination-pattern xxxx..... #Customer specific destination pattern
     session protocol sipv2
     session target ipv4:###.###.###.###     #IP Address for Unified CVP1, SideA
     session transport tcp
     voice-class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad



dial-peer voice 70023 voip
     description Used for Switch leg SIP Direct
     preference 2
     max-conn 225
     destination-pattern xxxx..... #Customer specific destination pattern
     session protocol sipv2
     session target ipv4:###.###.###.###    #IP Address for Unified CVP1, SideB
     session transport tcp
     voice-class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad
```

Step 7 Configure the hardware resources (transcoder, conference bridge, and MTP):

Note This configuration section is unnecessary for virtual CUBE or CSR 1000v Gateways. They do not have physical DSP resources.

```
#For gateways with physical DSP resources, configure Hardware resources using
#Unified Communications Domain Manager.

# Configure the voice-cards share the DSP resources located in Slot0
voice-card 0
     dspfarm
     dsp services dspfarm
voice-card 1
     dspfarm
     dsp services dspfarm
voice-card 2
     dspfarm
     dsp services dspfarm
voice-card 3
     dspfarm
     dsp services dspfarm
voice-card 4
     dspfarm
     dsp services dspfarm

# Point to the contact center call manager
sccp local GigabitEthernet0/0
     sccp ccm ###.###.###.### identifier 1 priority 1 version 7.0 # Cisco Unified CM sub 1
     sccp ccm ###.###.###.### identifier 2 priority 1 version 7.0 # Cisco Unifed CM sub 2

# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
     associate ccm 1 priority 1
     associate profile 2 register <gw70mtp>
     associate profile 1 register <gw70conf>
     associate profile 3 register <gw70xcode>

# Configure DSPFarms for Conference, MTP and Transcoder

dspfarm profile 1 conference
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions 24
     associate application SCCP

dspfarm profile 2 mtp
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions software 500
     associate application SCCP

dspfarm profile 3 transcode universal
     codec g711ulaw
     codec g711alaw
     codec g729r8
     maximum sessions 52
     associate application SCCP

# Note: Universal transcoder is only needed for cases where you engage the G.729 caller to
G.729 only agent with IVR in middle and performs any supplementary services or use features
like whisper announcement or agent greeting.
```

Step 8 Optional, configure the SIP Trunking:

```
# Configure the resources to be monitored
voice class resource-group 1
     resource cpu 1-min-avg threshold high 80 low 60
     resource ds0
     resource dsp
     resource mem total-mem
     periodic-report interval 30

# Configure one rai target for each CVP Server
sip-ua
     rai target ipv4:###.###.###.### resource-group1 # CVP1A
     rai target ipv4:###.###.###.### resource-group1 # CVP2A
     rai target ipv4:###.###.###.### resource-group1 # CVP1B
     rai target ipv4:###.###.###.### resource-group1 # CVP2B
     permit hostname dns:%Requires manual replacement - ServerGroup Name defined in
CVP.System.SIP Server Groups%
```

Step 9 Configure incoming PSTN SIP trunk dial peer:

```
dial-peer voice 70000 voip
     description Incoming Call From PSTN SIP Trunk
     service survivability
     incoming called-number xxxx……    # Customer specific incoming called-number pattern
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     session protocol sipv2
     voice class codec 1
     no vad
```

Configure VXML Gateway

Before you begin

Note If you have configured VVB, it is not mandatory to configure VXML Gateway. You may configure either VVB or VXML Gateway, or configure both.

Procedure

Step 1 Configure global settings:

```
voice service voip
sip
     rel1xx disable
     header-passing
     options-ping 60
     midcall-signaling passthru
```

Step 2 Configure default Unified CVP services:

```
#Default CVP Services
application
     service new-call flash:bootstrap.vxml
     service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
```

```
     service ringtone flash:ringtone.tcl
     service cvperror flash:cvperror.tcl
     service bootstrap flash:bootstrap.tcl
```

Step 3 Configure dial-peers:

Note While configuring VXML gateway voice class codec must not be used. G711ulaw may be used in general for the dial-peers, but still depending on the implementation the other codec may be used.

```
# Configure Unified CVP Ringtone
dial-peer voice 919191 voip
     description CVP SIP ringtone dial-peer
     service ringtone
     incoming called-number 9191T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

# Configure Unified CVP Error
dial-peer voice 929292 voip
     description CVP SIP error dial-peer
     service cvperror
     incoming called-number 9292T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

Step 4 Configure default Unified CVP HTTP, ivr, rtsp, mrcp and vxml settings:

```
http client cache memory pool 15000
http client cache memory file 1000
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client connection idle timeout 10
http client response timeout 30
ivr prompt memory 15000
ivr asr-server rtsp://asr-en-us/recognizer
ivr tts-server rtsp://tts-en-us/synthesizer
rtsp client timeout connect 10
rtsp client timeout message 10
mrcp client timeout connect 10
mrcp client timeout message 10
mrcp client rtpsetup enable
vxml tree memory 500
vxml audioerror
vxml version 2.0
```

Step 5 Configure primary and secondary media servers:

```
#Configure the media servers where
# the primary matches the default media server defined in OAMP.
# the secondary is located on the opposite side of the primary.

ip host mediaserver ###.###.###.###          # IP Address for primary media server.
ip host mediaserver-backup ###.###.###.###   # IP Address for secondary media server.
```

Step 6 Configure VXML leg where the incoming called-number matches the Network VRU Label:

```
dial-peer voice 7777 voip
     description Used for VRU leg
```

```
     service bootstrap
     incoming called-number 777T
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

Step 7 Configure ASR TTS:

```
#Configure primary server
ip host asr-en-us <ASR server ip>
ip host tts-en-us <TTS server hostname>
voice class uri TTS sip
pattern tts@<TTS server ip>
voice class uri ASR sip
pattern asr@<ASR server hostname>
ivr asr-server sip:asr@<ASR server hostname*>
ivr tts-server sip:tts@<TTS server hostname*>

dial-peer voice 5 voip
     description FOR ASR calls
     preference1
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     session target ipv4:<ASR server IP>
     destination uri ASR
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

dial-peer voice 6 voip
     description FOR TTS calls
     preference1
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     session target ipv4:<TTS server IP>
     destination uri TTS
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad

#Configure backup server
dial-peer voice 7 voip
     destination uri ASR
     session target ipv4:<ASR backup server IP>
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry
     2dtmf-relay rtp-nte
     codec g711ulaw
     preference 2
     no vad

dial-peer voice 8 voip
     destination uri TTS
     session target ipv4:<TTS backup server IP>
     session protocol sipv2
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry
     2dtmf-relay rtp-nte
     codec g711ulaw
     preference 2
     no vad
```

Step 8 Exit configuration mode and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the transferred Unified CVP files into the Cisco IOS memory for each Unified CVP service:

- call application voice load new-call
- call application voice load CVPSelfService
- call application voice load ringtone
- call application voice load cvperror
- call application voice load bootstrap
- call application voice load handoff

Configure Unified Communications Manager

Follow this sequence of tasks to configure Unified Communications Manager:

Sequence	Task	Done?
1	Configure Unified Communications Manager Publisher, on page 58	
2	Configure Unified Communications Manager Subscriber, on page 59	
3	Install VMware Tools for Windows, on page 68	
4	Unified Communications Manager License, on page 60	
5	Activate Services , on page 61	
6	Validate Clusterwide Domain Configuration, on page 62	
7	Upgrade Cisco JTAPI Client on PG, on page 30	
8	Configure SNMP, on page 90	

Configure Unified Communications Manager Publisher

You must customize the Unified Communications Manager publisher before you customize the subscribers.

Before you begin

Ensure that the Virtual Machine device status shows **Connect at Power On** checked for the Network adapter and Floppy drive.

Procedure

Step 1 Power on the Publisher. This begins the installation based on the information in the .flp file.The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the Publisher machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

Note During the customization of the publisher/primary, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: `c1sco@123`
- Application UserName: `Administrator`
- Default Password for Application User: `c1sco@123`
- Sftp password: `c1sco@123`
- IPSec password: `c1sco@123`

Configure Unified Communications Manager Subscriber

Launch Unified Communications Manager Publisher to Add the Subscriber

To add the subscriber, you must launch the publisher node.

Procedure

Step 1 Launch the Unified Communications Manager Publisher in a browser (http://<IP Addr of CUCM Publisher>/ccmadmin).

Step 2 Enter the username and password and login to the Unified Communications Manager.

Step 3 Select **System** > **Server** > **Add New**.

Step 4 On the Add a Server page, choose **CUCM Voice/Video** for the server type. Click **Next**.

Step 5 On the Server Information page, enter the IP address of the first subscriber.

Step 6 Click **Save**.

Step 7 Repeat Steps 3 - 6 for the second subscriber.

Configure Subscriber

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Subscriber.
This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUCM Secondary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the subscriber node, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **c1sco@123**
- Application UserName: **Administrator**
- Default Password for Application User: **c1sco@123**
- Sftp password: **c1sco@123**
- IPSec password: **c1sco@123**

Unified Communications Manager License

To configure the Unified Communications Manager license, first add a product instance, then generate and register the license, and then install the license.

Upgrade Unified Communications Manager License

Procedure

Step 1 Unzip the license file from the email message.

Step 2 Launch Unified Communications Manager in a browser (`https://<IP Address of CUCM Publisher>`).

Step 3 Click **Cisco Prime License Manager** and navigate to **Licenses** > **Fulfillment**.

Step 4 Under Other Fulfillment Options, select **Fulfill Licenses from File**.

Step 5 Click **Browse** and locate your license file.

Step 6 Click **Install** and close the popup window.

Step 7 Navigate to **Product Instances**. Delete any old instances. Then click **Add**.

Step 8 Fill in the name, hostname/IP address, username, and password for your Cisco Unified Communications Manager Publisher.

Step 9 Select Product type of Unified CM.

Step 10 Click **OK**.

Step 11 Click **Synchronize Now**.

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

Complete the following procedure to install a license.

Procedure

Step 1 Unzip the license file from the email message.

Step 2 Navigate to **License Management > Licenses**.

Step 3 Under Other Fulfillment Options, choose **Fulfill Licenses from File**.

Step 4 Browse for the license file and click **Install**.

Step 5 Navigate to the **Monitoring > License Usage** page to verify a successful installation.

Activate Services

Complete the following procedure to activate services.

Procedure

Step 1 Launch the Unified Communications Manager in a browser (http://<IP Address of CUCM Node>).

Step 2 From the Cisco Unified Serviceability drop-down list, choose **Tools** > **Service Activation**.

Step 3 From the Server drop-down list, choose the server on which you want to activate the services, and then click **Go**.

The window displays the service names and activation status of the services.

Step 4 Check the following services to activate:

a) Publisher:

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

b) Subscriber:

- Subscriber's for call processing
  - Cisco CallManager
  - Cisco IP Voice Media Streaming App
  - Cisco CTIManager
  - Cisco CTL Provider
  - Cisco AXL Web Service
- Subscriber's for TFTP and Music on Hold

  Note Enable TFTP Service in Publisher node for HCS for CC deployments that doesn't have a dedicated TFTP and MoH server.

  - Cisco TFTP
  - Cisco IP Voice Media Streaming App

Step 5 Click **Save**.

Note Activating Cisco CallManager, will automatically Activate CTIManager and Cisco Dialed Number Analyzer server. Click **OK** when prompted.

Validate Clusterwide Domain Configuration

This validation is required for running calls.

Procedure

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

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

Cluster Fully Qualified Domain Name should match the Server Group name in the Unified CVP SIP Server Groups Configure SIP Server Group, on page 49.

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 63 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.

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 64.

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.

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.

Configure Unified Intelligence Center Coresident Deployment

Sequence	Task	Done?
1	Configure Unified Intelligence Center Publisher, on page 65	
2	Configure Unified Intelligence Center Subscriber, on page 66	
3	Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory, on page 67	
4	Install VMware Tools for Windows, on page 68	
5	Configure Unified Intelligence Center Reporting, on page 68	
6	Configure Unified Intelligence Center Administration, on page 71	
7	Configure SNMP, on page 90	
8	Configure Live Data AW-Access, on page 73	
9	Configure Live Data Unified Intelligence Data Sources, on page 75	
10	Configure Live Data Reporting Interval, on page 76	
11	Configure Transport Layer Security , on page 76	
12	Import Reports, on page 41	
13	Add Certificate for HTTPS Gadget, on page 78	

Configure Unified Intelligence Center Publisher

You must customize the Cisco Unified Intelligence Center publisher before you customize the subscriber.

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Publisher.

This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUIC Primary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the publisher/primary, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **c1sco@123**
- Application UserName: **Administrator**
- Default Password for Application User: **c1sco@123**
- Sftp password: **c1sco@123**
- IPSec password: **c1sco@123**

Configure Unified Intelligence Center Subscriber

Follow the below steps to for both CUIC with Live data and Live Data stand-alone deployment:

Note Ensure that the license is updated before adding the subscriber node.

Launch Publisher to Add Subscriber

Procedure

Step 1 Enter `http://<HOST ADDRESS>/oamp` URL in the browser, where *HOST ADDRESS* is the IP Address or 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 left panel, choose **Device Management** > **Device Configuaration**.

Step 4 Click **Add Member**.

Step 5 Enter hostname or IP address in **Name** field.

Step 6 Enter **Description** for the device.

Step 7 Click **Save**.

Configure Subscriber

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Subscriber.
This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUIC Secondary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the subscriber node, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **`c1sco@123`**
- Application UserName: **`Administrator`**
- Default Password for Application User: **`c1sco@123`**
- Sftp password: **`c1sco@123`**
- IPSec password: **`c1sco@123`**

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

Procedure

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

Step 2 Add the new machine to the System Inventory:

a) Click **Add**.

The **Add Machine** popup window opens.

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

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

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

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

d) Enter the machine's Administration credentials.

e) Click **Save**.

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

What to do next

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

Install VMware Tools for Windows

Procedure

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

Step 2 Click the **Summary** tab.

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

- installed and current
- installed and not current
- not installed

Step 3 Click the **Console** tab to make sure that the guest operating system starts successfully. Log in if prompted.

Step 4 Right-click the virtual machine, select **Guest OS**, and then click **Install/Upgrade VMware Tools**. The **Install/Upgrade VMware Tools** window appears with the option - Interactive Tools Upgrade and Automatic Tools Upgrade.

a) To install/upgrade the VMware tools manually, select the **Interactive Tools Upgrade** option, and click **OK**. Follow the on-screen instructions to install/upgrade the VMware tools, and restart the virtual machine when prompted.

b) To install/upgrade the VMware tools automatically, select the **Automatic Tools Upgrade** option, and click **OK**. This process takes a few minutes to complete, and restart the virtual machine when prompted.

Configure Unified Intelligence Center Reporting

Complete the following procedures to configure Unified Intelligence Center Reporting.

Configure the SQL User Account

Complete the following procedure on both sides of the Unified CCE Historical database servers and the Unified CCE Real-time database servers to allow SQL authentication and to enable TCP/IP protocol and remote network connections.

Procedure

Step 1 Log in to the Unified CCE Historical and Real-time database servers in your deployment.

Step 2 Open **SQL Server Management Studio**.

Step 3 Login using default credentials.

Step 4 Expand **Security** tab. Right-click **Logins** and choose **New Login**.

Step 5 In **General** page, enter the following values:

a) Enter **Login Name**.

Example:

user

b) Choose **SQL Server authentication**.
c) Enter **Password** and re-enter the password to confirm.
d) Uncheck **Enforce password policy** check box.

Step 6 In **Server Roles** page, check the following check boxes:

- **public**
- **securityadmin**
- **serveradmin**
- **setupadmin**
- **sysadmin**

Step 7 In **User Mapping** page, enter the following values:

a) Check the **Real-time database** and **Historical database** check boxes .
b) In **Database role memberships** pane, check the following check boxes:

- **db_datareader**
- **db_datawriter**
- **db_ddladmin**
- **db_owner**
- **db_securityadmin**
- **public**

Step 8 Click **OK**.

Configure Unified Intelligence Center Data Sources

Complete the following procedure to allow Unified Intelligence Center to configure Unified CCE Historical Data source and Unified CCE Real-time Data source.

Note You can distribute the reporting load to several Unified CCE AW_HDS databases using the command line interface and conventional name resolution. If there is a need to direct a specific member node to a database host other than the one in configured on the data sources interface, you can use the "set cuic-properties host-to-ip" command to resolve the data source name differently on each node.

Procedure

Step 1 Login to Unified Intelligence Center portal as administrator (http://{hostname})

Step 2 From the navigation pane, click **Configure > Data Sources**.

Step 3 Choose the **Unified CCE Historical** Data Source. Click **Edit** from the ellipsis to open the Data Source page. In the Primary tab, enter the following values

a) In the Datasource Host field, enter the hostname/IP address of the primary historical database server **(AW-HDS-A1).**
b) In the **Port** field, enter 1433 which is a port used for SQL server database.
c) In the **Database Name** field, enter the primary historical database name.
d) In the **Instance** field, leave blank as it is optional for SQL server.
e) In the **Timezone** field, select the time zone for the data stored in the database.
f) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
g) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
h) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
i) In the **Permissions** pane, accept the default values

Step 4 Click on the **Secondary** tab and enter the following values.

a) Check **Failover Enabled**
b) In the Datasource Host field, enter the hostname/IP address of the secondary historical database server **(AW-HDS-B1)**.
c) In the **Port** field, enter 1433 which is a port used for SQL server database.
d) In the **Database Name** field, enter the secondary historical database name.
e) In the **Instance** field, leave blank as it is optional for SQL server.
f) In the **Timezone** field, select the time zone for the data stored in the database.
g) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
h) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
i) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
j) In the **Permissions** pane, accept the default values.

Step 5 Click **Test Connection** to ensure the data source is online and click **Save** .

Step 6 Choose the **Unified CCE Realtime** Data Source. Click **Edit** to open the **Data Source** > **Edit** page. In the Primary tab, enter the following values.

a) In the Datasource Host field, enter the hostname/IP address of the primary realtime database server **(AW-HDS-A2).**
b) In the **Port** field, enter 1433 which is a port used for SQL server database.
c) In the **Database Name** field, enter the primary realtime database name.
d) In the **Instance** field, leave blank as it is optional for SQL server.
e) In the **Timezone** field, select the time zone for the data stored in the database.
f) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
g) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
h) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
i) In the **Permissions** pane, accept the default values

Step 7 Click on the **Secondary** tab and enter the following values.

a) Check **Failover Enabled**.

b) In the Datasource Host field, enter the hostname/IP address of the secondary realtime database server **(AW-HDS-B2)**.
c) In the **Port** field, enter 1433 which is a port used for SQL server database.
d) In the **Database Name** field, enter the secondary realtime database name.
e) In the **Instance** field, leave blank as it is optional for SQL server.
f) In the **Timezone** field, select the time zone for the data stored in the database.
g) In the **Database User ID** field, enter the SQL user account created earlier for CUIC to access the database.
h) In the **Password** and **Confirm Password** fields, enter the password for SQL user account.
i) In the **Charset** drop-down field, choose **ISO-8859-1** (Latin 1 encoding)
j) In the **Permissions** pane, accept the default values

Step 8 Click **Test Connection** to ensure the data source is online and click **Save**.

What to do next

After configuring Unified Intelligence Center, you can import stock templates using the Import functionality and customize the stock reports based on your requirements. The stock templates are designed to present Unified CCE /CC data. Navigate to User Guide for the Cisco Unified Intelligence Center Reporting Application. Under Chapter **Reports** see section **Stock Report Templates** to import Unified CCE Report templates.

Configure Unified Intelligence Center Administration

Complete the following procedure to configure Unified Intelligence Center Administration.

Procedure

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

Step 2 Configure the Active Directory tab under **Cluster Configuration > Reporting Configuration**.

a) For Host Address for the Primary Active Directory Server, enter the IP address of the domain controller.
b) For Port, enter the port number for the domain controller.
c) Complete the **Manager Distinguished Name** fields that are required for the customer.
d) Enter and confirm the password with which the Manager accesses the domain controller.
e) For User Search Base, specify users and the domain name and any sub-domain names .
f) For Attribute for User ID, select the required option.

Note If the Windows domain name and the NETBIOS names are different, do the following: in the **Cisco Unified Intelligence Center Administration Console**, under **Active Directory Settings**, in the field **Attribute for User ID**, ensure to select *sAMAccountName*, and add the *NETBIOS* value to set it as default value.

g) Add at least one domain for the UserName Identifier. Do not type the @ sign before the domain name.
h) Set a domain as the default.
i) Click **Test Connection**.
j) Click **Save**.

Note For more details, see the online help.

Step 3 Configure syslog for all devices.

a) Choose **Device Management** > **Logs and Traces Settings**.

b) For each host address:

- Select the associated servers and click the arrow to expand.
- Select the server name.
- In the **Edit Serviceability Settings** screen **Syslog Settings** pane, configure the Primary and Backup Host. Click **Save**.

Step 4 Configure SNMP for all devices, if used.

a) Select **Network Management** > **SNMP**.

b) Navigate to SNMP and for each server add the following:

- V1/V2c Community Strings.
- Notification Destination.

Unified Intelligence Center License and Sign-In

Sign In to Administration Console

Who can sign in to the administration console: The System Application User who is the default Superuser.

To upload the license, you must sign in to the Unified Intelligence Center Administration Console. This is the OAMP interface for Unified Intelligence Center. The first person who signs in to the Administration application must do so using the user ID and password that were defined for the System Application User during the installation. This user is the initial Superuser for Unified Intelligence Center Administration.

Procedure

Step 1 Enter this URL: `http://<HOST ADDRESS>/oamp`, where HOST ADDRESS is the IP address or hostname of your Controller node.

Step 2 Enter the System Application User ID and password that you defined during installation.

Upload License

Who can upload the license: The System Application User who is the default Superuser.

As soon as the System Application User signs in, the user must upload the license file. The file is uploaded to the Controller publisher node and, within a minute, is automatically replicated to all nodes in the cluster.

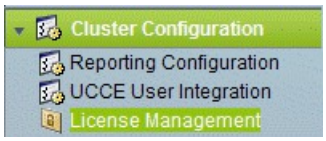
The partner must obtain a unique license and apply it to the imported Unified Intelligence Center servers at the customer site.

Procedure

Step 1 In Cisco Unified Intelligent Center Administration, choose **Cluster Configuration** > **License Management**.

to open the **License File Management** page.

Figure 1: License File Management



Step 2 Click **Browse**.

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

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

A message appears indicating that the license file was uploaded successfully and will be distributed to other nodes (if any) in the cluster in approximately one minute.

Note The databases are polled once a minute for changes. The license replication is not immediate but occurs within a minute.

What to do next

Create Reporting Users, on page 38

Configure Live Data AW-Access

Live Data AW DB access commands allow you to configure and view Unified CCE AW DB (real-time distributor) access for Unified CCE Live Data Product Deployment Selection. You can also test the connection.

Procedure

Step 1 Log in to **CUIC Live Data Console** and run the following command:

set live-data aw-access primary *addr port db user pwd* [*test*]

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

Table 6: Command Description

Command	Description	Example
addr	Specifies the hostname or IP address of the primary or secondary Unified CCE AW (Maximum 255 characters).	10.10.10.10 or AWmachinename.domain.com
port	Specifies the listening port of the database server (ranges 1-65535).	1433 db

Command	Description	Example
db	Specifies the database name (maximum 128 characters).	inst_awdb
user	Specifies the login user (maximum 128 characters) For more information about creating user, see Configure the SQL User Account , on page 68	user
pwd	Specifies the login password (maximum 128 characters).	password
test	This parameter is optional. Tests the connection to the primary or secondary AW DB. Checks weather AW DB access for configured users and provides the results.	

Step 2 Run the following command to view the primary and secondary Unified CCE AW DB access information. Optional, test the connection from Live Data to each AW DB, check if configured user (on each node) has appropriate AW DB access:

show live-data aw-access primary *addr port db user pwd* [*test*]

show live-data aw-access secondary *addr port db user pwd* [*test*]

Configure Live Data Machine Services

Procedure

Step 1 Log in to **CUIC Live Data Console**.

Step 2 Run the below command to configure the latest information from Live Data with Machine Service table.

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

Note This command is not valid for coresident deployments. If you have a coresident deployment, use the System Inventory in the Unified CCE Administration tool.

Table 7: Command Description

Command	Description	Example
awdb-user	Specifies the AW database domain user, who has write-access permission.	administrator@domain.com
awdb-pwd	Specifies the AW database user password.	password

Step 3 Run the below command to view Live Data entries in the **Machine Services** table:

`show live-data machine-services` *awdb-user awdb-pwd*

Note Enter FQDN host name in correct format. The machine (host) name must start with an alphanumeric character string with a maximum length of 32 characters. The machine name allows only characters such as period (.), underscore (_), dash (-), and alphanumeric characters. If the host name contains invalid characters or the name exceeds 32 characters, an error message appears.

Step 4 After you updated the host name of the Live Data Server, you must re-run the following commands, to update the Live Data machine services with the new host name.

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

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

Configure Live Data Unified Intelligence Data Sources

Before you begin

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

Procedure

Step 1 Run the following command to configure the data source of Live Data in Cisco Unified Intelligence Center:

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

Table 8: Command Description

Command	Description	Example
cuic-addr	Specifies the Cisco Unified Intelligence Center publisher node's Fully Qualified Domain Name (FQDN).	10.10.10.10 or CUIC + LiveDatamachinename.domain.com **Important** Given node should be in service.
cuic-port	Specifies the Cisco Unified Intelligence Center REST API port. Typically this port is 8444.	
cuic-user	Specifies the user name to use for authentication with Cisco Unified Intelligence Center. By default, Cisco Unified Intelligence Center requires that you specify **CUIC** as the domain with the user name.	`CUIC\administrator`
cuic-pwd	Specifies the password to use for authentication with Cisco Unified Intelligence Center.	password

Step 2 Run the following command to display Data Source:

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

Configure Live Data Reporting Interval

Procedure

Step 1 Log in to **CUIC Live Data Console**.

Step 2 Run the following command to set Live Data reporting interval in minutes format:

```
set live-data reporting-interval reporting-interval-in-minutes
```

Table 9: Command Description

Command	Description	Example
reporting-interval-in-minutes	Specifies the reporting interval in minutes format. The valid values are 5, 10, 15, 30, and 60 minutes.	5

Step 3 After Live Data reporting interval is set, run the below command to restart the publisher and subscriber node (Restart the inactive node first and active node next):

```
utils system restart
```

Step 4 Run the below command to view Live Data reporting interval:

```
show live-data reporting-interval
```

Configure Transport Layer Security

Follow the procedures to set TLS Server and TLS Client minimum version.

Import Reports

You can import the Unified Intelligence Center report, which is in either .xml or .zip file format.

The imported report retrieves data for the following entities:

- Report
- Report Definition
- Value Lists
- Views

- Thresholds
- Drilldowns
- Template Help

Note Each report template help folder has a size limit of 3 MB. If the folder size exceeds this limit, the system does not load the help content.

Note You cannot import Report Filters and Collections.

Ensure that the data source is used to import the Report Definition is configured in Unified Intelligence Center. Also, ensure that data source is used by any value list that is defined in Unified Intelligence Center, if the report definition has any value list defined.

To import reports, perform the following steps:

Procedure

Step 1 In the left navigation pane, choose **Reports**.

Step 2 In the **Reports** listing page, click **Import**.

Step 3 Click **Browse** to select the file (.xml or .zip format) to be imported.

Note Maximum file size for .zip file format is 60 MB and for .xml file format is 3 MB.

Step 4 Select the required file and click **Open**.

Step 5 Select the file location from the **Save to Folder** list to save the file.

Step 6 Click **Upload**.
Once the file is successfully uploaded, the table gets populated with the corresponding report template, current available version, and incoming version of the files being imported.

Step 7 Select a Data Source for the Report Definition only if the Report Definition for the report being imported is not defined in Unified Intelligence Center.

Step 8 Select a Data Source for the Value List that is defined in the Report Definition.

Note Selection of a Data Source for the Value List is mandatory:

- If the Value List does not use the same Data Source as the Report Definition.
- For Real Time Streaming Report Definitions.

Step 9 Select the files to import or overwrite.

- Overwrite—If the report being imported exists in the Unified Intelligence Center.
- Import—If the report being imported is the new set of report files.

Step 10 Click **Import**.

Note
- Importing a report to a different version of Unified Intelligence Center is not supported. However, when you upgrade Unified Intelligence Center, report templates continue to work in the upgraded version.
- Importing manually edited XMLs is not supported.

Add Certificate for HTTPS Gadget

Add a certificate for a secure HTTP (HTTPS) gadget to allow the gadget to load into the Finesse desktop and successfully perform HTTPS requests to the Finesse server.

This process allows HTTPS communication between the Finesse gadget container and the third-party gadget site for loading the gadget and performing any API calls that the gadget makes to the third-party server.

Note A gadget that loads using HTTPS may still use HTTP communication between that gadget and the application server where it resides. If all traffic must be secure, the gadget developer must ensure that HTTPS is used to make API calls to the application server.

The certificate must be signed with a common name. The gadget URL in the desktop layout must use the same name (whether it uses an IP address or a fully qualified domain name) as the name with which the certificate is signed. If the certificate name and the name in the gadget URL do not match, the connection is not trusted and the gadget does not load.

Before you begin

Set up security certificates for finesse, Cisco Unified Intelligence Center and Live Data server to server communication. Import certificates into servers as shown in the table below:

Server	Import Certificates
Finesse	Live Data and Cisco Unified Intelligence Center
Cisco Unified Intelligence Center	Live Data

Procedure

Step 1 Download the tomcat-trust.pem certificate from the third-party gadget host.

a) Sign in to Cisco Unified Operating System Administration on the third-party gadget host (`http://host or IP address/cmplatform` where `host` or `IP address` is the hostname or IP address of third-party gadget host).
b) Choose **Security** > **Certificate Management**.
c) Click **Find**.
d) Click **Common Name** hyperlink for the required tomcat trust.
e) Click **Download.PEM File**.

Step 2 Upload the certificate to the Finesse Publisher server.

a) Sign in to Cisco Unified Operating System Administration on Finesse Publisher server (`http://host or IP address/cmplatform` where `host` or `IP address` is the hostname or IP address of the finesse server).
b) Choose **Security** > **Certificate Management**.
c) Click **Upload Certificate**.
d) Choose **Tomcat Trust** from **Certificate Purpose** drop-down list.
e) Click **Common Name** hyperlink for the required tomcat trust.
f) Click **Browse** to choose the downloaded tomcat-trust.pem file.
g) Click **Upload File**.

Step 3 Restart **Cisco Tomcat** and **Cisco Finesse Tomcat** services on the Finesse Publisher server.

Step 4 Ensure the certificates are synchronized in Finesse Subscriber server.

Step 5 Restart **Cisco Tomcat** and **Cisco Finesse Tomcat services** on Finesse Subscriber server.

Configure Cisco Finesse

This table lists the configuration procedures for Cisco Finesse:

Sequence	Task	Done?
1	Configure the Cisco Finesse Primary Node, on page 79	
2	-	
3	Configure Cisco Finesse Secondary Node, on page 84	
4	Install VMware Tools for Windows, on page 68	
5	Configure Cisco Finesse Administration, on page 85	
6	Configure SNMP, on page 90	

Configure the Cisco Finesse Primary Node

Note You must configure the Cisco Finesse primary node before you customize the secondary node.

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the primary node. To begin the installation based on the information in the .flp file.

The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the Finesse Primary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power** on for the floppy drive.

Note During the customization of the primary, the username and the password are modified as follows. The customer should change the password.

- Default Password for OS Administrator: **c1sco@123**
- Application UserName: **Administrator**
- Default Password for Application User: **c1sco@123**
- Sftp password: **c1sco@123**
- IPSec password: **c1sco@123**

After rebooting, the VM installation is complete with all the parameters provided in the spreadsheet for the VM.

Configure Settings for the CTI Server and Administration and Data Server

- Configure Contact Center Enterprise CTI Server Settings in the Cisco Finesse Primary Node, on page 80
- Configure Contact Center Enterprise Administration and Data Server Settings, on page 83
- Restart the Cisco Tomcat Service, on page 83

Configure Contact Center Enterprise CTI Server Settings in the Cisco Finesse Primary Node

Access the administration console on the primary Finesse server to configure the A and B Side CTI servers.

Note After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, wait for 6 minutes before you attempt to access the Finesse administration console.

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

Procedure

Step 1 Sign in to the administration console on the primary Finesse server:

http://*FQDN of Finesse server*/cfadmin

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

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

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

Step 4 Click **Save**.

Contact Center Enterprise Administration and Data Server Settings

Use the Unified CCE Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.

Note To connect to the AW Database (AWDB) in the Unified CCE Administration, Cisco Finesse supports both SQL and Windows authentication.

The Cisco Finesse Java Database Connectivity (JDBC) driver is configured to use NTLMv2. Therefore, Finesse can connect to the administration database even if the administration database is configured to use only NTLMv2.

Primary Administration & Data Server is configured on Side A and Secondary Administration & Data Server is configured on Side B. Make sure Cisco Finesse server on both sides connect to Primary Administration & Data Server on side A and fall back to Secondary Administration & Data Server on side B only when Primary Administration & Data Server goes down.

After you change and save any value on the Contact Center Enterprise Administration & Data Server Settings gadget, restart the Cisco Finesse Tomcat Service on the primary and secondary Finesse server. If you restart the Cisco Finesse Tomcat Service, agents must sign out and sign in again. To avoid this, you can make Contact Center Enterprise Administration & Data Server settings changes and restart the Cisco Finesse Tomcat service during hours when agents are not signed in to the Cisco Finesse desktop.

The following table describes the fields on the Unified CCE Administration & Data Server Settings gadget:

Table 10: Field Descriptions

Field	Description
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server.
Backup Host/IP Address	(Optional) The hostname or IP address of the backup Unified CCE Administration & Data Server.
Database Port	The port of the Unified CCE Administration & Data Server. The default value is 1433. **Note** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
AW Database Name	The name of the AW Database (AWDB). For example, *ucceinstance*_awdb).
Domain	(Optional) The domain name of the AWDB.
Username	The username required to sign in to the AWDB. **Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user. If you do not specify a domain, this user must be an SQL user.
Password	The password required to sign in to the AWDB.

For more information about these settings, see the *Administration Guide for Cisco Unified Contact Center Enterprise* and the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise*.

Actions on the Unified CCE Administration & Data Server Settings gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved enterprise database settings

When you update any of the following fields and click Save, Cisco Finesse attempts to connect to the AWDB:

- Primary Host/IP Address
- Backup Host/IP Address
- Database Port
- AW Database Name

If Cisco Finesse cannot connect to the AWDB, an error message appears and you are asked if you still want to save. If you click **Yes**, the settings are saved. If you click **No**, the settings are not saved. You can change the settings and try again or click **Revert** to retrieve the previously saved settings.

When you update the Username or Password fields and click **Save**, Cisco Finesse attempts to authenticate against the AWDB. If authentication fails, an error message appears and you are asked if you still want to save. Click **Yes** to save the settings or click **No** to change the settings. Click **Revert** to retrieve the previously saved settings.

Note Finesse will not come into service in case of AWDB errors when connecting Cisco Finesse 11.5(1) and higher versions to Unified CCE 11.5(1) and higher versions.

Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Unified CCE Administration & Data Server settings to enable authentication for Finesse agents and supervisors.

Procedure

Step 1 If you are not already signed in, sign in to the administration console.

Step 2 In the Unified CCE Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the preceding table. For more information, see Table 10: Field Descriptions, on page 82. Refer to your configuration worksheet if necessary.

Step 3 Click **Save**.

What to do next

The CTI test functionality documented in the *Configure Unified CCE CTI Server Settings* topic depends on AWDB connectivity to determine the CTI version. Or else, the test will not go through.

Restart the Cisco Tomcat Service

After you change and save any value on Unified CCE Administration server settings, you must restart the Cisco Tomcat Service on the primary Cisco Finesse server.

Procedure

Step 1 Enter **utils service stop Cisco Tomcat** command, to stop the Cisco Tomcat service.

Step 2 Enter **utils service start Cisco Tomcat** command, to start the Cisco Tomcat service.

Configure Cisco Finesse Secondary Node

Launch the Finesse Administration Console to Configure the Secondary Finesse

To add the secondary node, you must launch the primary node and add the secondary node to the cluster.

Procedure

Step 1 Launch the Cisco Finesse primary node in a browser (`http://Primary Node FQDN/cfadmin`), where the primary node or IP address is that of your host.

Step 2 Select **Settings** > **Cluster Settings**. (Cluster settings are based on the default configuration and assumes that you have not changed the page for the Cluster Settings tool.)

Step 3 Add the IP address for the Cisco Finesse secondary node.

Step 4 Click **Save**.

Step 5 Restart Cisco Tomcat as follows:

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

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

Install Cisco Finesse on the Secondary Node

Before you begin

Ensure that you select the **Connect at Power on** check box of the virtual machine for network adapter and floppy drive.

Procedure

Step 1 Power on the secondary node to begin the installation based on the information in the .flp file.
The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the virtual machine. Log into the Cisco Finesse secondary machine, using the credentials for the administration user. The machine opens to the CLI interface.

Step 3 Right-click the virtual machine and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

Note During the customization of the secondary node, the username and the password is modified as follows. You can change the password:

- Default password for OS Administrator: **c1sco@123**
- Application username: **Administrator**
- Default password for application user: **c1sco@123**
- Sftp password: **c1sco@123**
- IPsec password: **c1sco@123**

Configure Cisco Finesse Administration

- Obtain and Upload CA Certificate, on page 85
- Accept Security Certificates, on page 87

Obtain and Upload CA Certificate

Note This procedure only applies if you are using HTTPS and is optional. If you are using HTTPS, you can choose to either obtain and upload a CA certificate or use the self-signed certificate provided with Finesse.

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a CA. Use the Certificate Management utility from Cisco Unified Operating System Administration.

To open Cisco Unified Operating System Administration in your browser, enter:

https://*FQDN of primary Finesse server*:8443/cmplatform

Sign in using the username and password for the Application User account created during Finesse installation.

Note You can find detailed explanations in the Security topics of the *Cisco Unified Operating System Administration Online Help*.

Procedure

Step 1 Generate a CSR.

a) Click **Security** > **Certificate Management** > **Generate CSR**.

b) From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.

Step 2 Download the CSR.

a) Select **Security** > **Certificate Management** > **Download CSR**.

b) From the Certificate Name drop-down list, choose **tomcat** and click **Generate CSR**.

Step 3 Generate and download a CSR for the secondary Unified CCX server.

To open Cisco Unified Operating System Administration for the secondary server in your browser, enter:

https://*FQDN of secondary Finesse server*:8443/cmplatform

Step 4 Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.

Note To set up the certificate chain, you must upload the certificates in the order described in the following steps.

Step 5 When you receive the certificates, click **Security** > **Certificate Management** > **Upload Certificate**.

Step 6 Upload the root certificate.

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

Step 7 Upload the intermediate certificate.

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

Step 8 Upload the application certificate.

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

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

Step 10 Access the CLI on the primary Finesse server.

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

Step 12 Enter the command **utils service restart Cisco Finesse Tomcat** to restart the Cisco Finesse Tomcat service.

Step 13 Upload the application certificate to the secondary Finesse server.

The root and the intermediate certificates uploaded to the primary server are replicated to the secondary server.

Step 14 Access the CLI on the secondary Finesse server and restart the Cisco Finesse Notification Service and the Cisco Finesse Tomcat Service.

Set Up CA Certificate for Chrome and Edge Chromium (Microsoft Edge) Browsers

Procedure

Step 1 In the browser, go to **Settings**.

Step 2 In the Chrome browser, select **Advanced Settings** > **Privacy and Security**, click **Manage Certificates**.

Step 3 In the Microsoft Edge browser, select **Privacy, search, and services**. Under **Security**, click **Manage Certificates**.

Step 4 Click **Trusted Root Certification Authorities** tab.

Step 5 Click **Import** and browse to the *ca_name*.cer file.
In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.

Step 6 Restart the browser for the certificate to install.

Accept Security Certificates

Ensure that the pop-ups are enabled for the Finesse desktop.

After you enter the Finesse desktop URL in your browser, the procedure to add a certificate is as follows:

Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

Internet Explorer

Note If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the security certificates. In your Start menu, right-click Internet Explorer and select Run as administrator.

Contact your administrator if you do not have the required permissions to install the security certificates.

1. A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open the Finesse sign in page. The Finesse sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. Select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users.
5. On the **Certificate Import Wizard**, click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
9. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
10. Click **OK** and close the **Certificate Import** dialog box.
11. Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Note To remove the certificate error from the desktop, you must close and reopen your browser.

Firefox

1. On **Your connection is not secure** page, click **Advanced** > **Add Exception**.

Note Ensure that the **Permanently store this exception** box is checked.

2. Click **Confirm Security Exception**.
3. On and click **Sign In**.
4. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
5. On the browser tab, click **I Understand the Risks** > **Add Exception**. Ensure that the **Permanently store this exception** box is checked.
6. Click **Confirm Security Exception**. The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Chrome and Edge Chromium (Microsoft Edge)

1. A page appears that states your connection is not private. To open the Finesse sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
4. On the browser tab,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

   The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Note If you click the certificate link and do not accept it, the certificate link stays enabled in the **SSL Certificate Not Accepted** dialog box. The certificate error appears every time you sign in. The procedure to permanently accept the certificate is as follows.

5. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (not valid)**.

   The **Certificate** dialog box appears.

6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (**.cer** file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.
12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

Close the browser and sign in to Finesse. The security error does not appear in the address bar.

Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

Chrome and Edge Chromium (Microsoft Edge)

1. A warning page appears which states that your connection is not private. To open the Finesse Console sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.
3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

Firefox

1. In your Firefox browser, enter the Finesse desktop URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.

Note If **.crt** file option is not available, select **.der** option to save the certificate.

4. From the menu, select **Firefox** > **Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

Configure SNMP

Procedure

Step 1 Log in to the Cisco Unified Serviceability *(https://hostname of primary server:8443/ccmservice)* using administrator credentials.

Step 2 Select **SNMP** > **V1/V2c** > **Community String**.

Step 3 From **Server** drop-down list, select the server for which you want to configure a community string and click **Find**.

Step 4 Click **Add New** to add new community string.

a) Enter **Community String**.

Example:

public.

b) In **Host IP Addresses Information** field, choose **Accept SNMP Packets from any host**.

c) From **Access Privilages** drop-down list, select **ReadWriteNotify** option.

d) Check **Apply to All Nodes** check box to apply community string to all nodes in the cluster.

Information message will be displayed.

e) Click **OK**.

f) Click **Save**.

A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.

g) Click **OK**.

Step 5 Select **SNMP** > **V1/V2c** > **Notification Destination**.

Step 6 From **Server** drop-down list, select the server for which you want to configure a notification destination and click **Find**.

Step 7 Click **Add New** button to add new notification destination.

a) From **Host IP Addresses** drop-down list, select **Add New**.
b) In **Host IP Address** field, enter the Prime Collaboration server IP address .
c) In the **Port Number** field, enter the notification receiving port number.

Note Default port number is 162.

d) In **SNMP Version Information** field, select the SNMP Version V2C.
e) In **Notification Type Information** field; from **Notification Type** drop-down list, select **Trap**.
f) In **Community String Information** field; from **Community String** drop-down list, select Community String created in Step 4 from the drop-down list.
g) Check the **Apply to All Nodes** check box to apply community string to all nodes.

Information message will be displayed.

h) Click **OK**.
i) Click **Insert**.

A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.

j) Click **OK**.

Create a Customer Instance for the 4000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 4000 agent for Cisco HCS for CC. After each task, return to this page to mark the task “done” and continue the sequence.

Table 11: Create customer instance for 4000 agent deployment of Cisco HCS for CC for Contact Center

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 2	
2	Set Up Virtual Machine Startup and Shutdown, on page 2	
3	Create a Domain Controller Server, on page 3	
4	Configure Cisco Unified CCE Rogger, on page 92	
5	Configure Unified CCE AW-HDS-DDS, on page 16	
6	Configure Unified CCE PG, on page 22	
7	Configure Unified CVP, on page 34	
8	Configure Cisco IOS Enterprise Voice Gateway, on page 52	
9	Configure Unified Communications Manager, on page 58	

Sequence	Task	Done?
10	Configure Unified Intelligence Center , on page 93	
11	Configure Live Data Reporting System, on page 102	
12	Configure Cisco Finesse, on page 79	
13	Configure Cisco Identity Service, on page 94	

Configure Cisco Unified CCE Rogger

This table lists the configuration procedures you must perform to configure Cisco Unified CCE Rogger.

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Verify the Machine in Domain, on page 9	
3	Configure the Domain Manager, on page 10	
4	Configure Unified CCE Encryption Utility, on page 11	
5	Configure SQL Server for CCE Components, on page 11	
6	Allocate a Second Virtual Hard Drive, on page 12	
7	Configure the Unified CCE Logger, on page 12	
8	Configure the Unified CCE Router, on page 15	
9	Load Base Configuration, on page 92	
10	Verify Cisco Diagnostic Framework Portico, on page 31	
11	Cisco SNMP Setup, on page 31	

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_11.6.1-Day1_4000.zip or file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Rogger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Rogger on Side A.

Step 5 Select the Unified CCE Rogger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Rogger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCEE Rogger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Rogger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start**. After synchronization click **OK**.

Configure Unified Intelligence Center

Follow these tasks to configure Unified Intelligence Center.

Sequence	Task	Done?
1	Configure Unified Intelligence Center Publisher, on page 65	
2	Configure Unified Intelligence Center Subscriber, on page 66	
3	Install VMware Tools for Windows, on page 68	
4	Configure Unified Intelligence Center Reporting, on page 68	
5	Configure Unified Intelligence Center Administration, on page 71	
6	Configure SNMP, on page 90	

Configure Live Data Reporting System

Sequence	Task	Done?
1	Configure Live Data AW-Access, on page 73	
2	Configure Live Data Machine Services, on page 74	

Sequence	Task	Done?
3	Configure Live Data Unified Intelligence Data Sources, on page 75	
4	Configure Live Data Reporting Interval, on page 76	
5	Configure Transport Layer Security , on page 76	
6	Import Reports, on page 41	
7	Add Certificate for HTTPS Gadget, on page 78	

Configure Cisco Identity Service

Sequence	Task	Done?
1	Configure Ids Publisher , on page 94	
2	Set IdS Subscriber Node, on page 94	
3	Configure Ids Subscriber , on page 95	

Configure Ids Publisher

You must customize the Cisco Identity Service publisher before you customize the subscribers.

Before you begin

Ensure that the Virtual Machine device status shows **Connect at Power On** checked for the Network adapter and Floppy drive.

Procedure

Step 1 Power on the Publisher. This begins the installation based on the information in the .flp file.The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the Publisher machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

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.

Configure Ids Subscriber

Before you begin

Ensure that the Virtual Machine device status is **Connect at Power On** checked for the Network adapter and Floppy drive

Procedure

Step 1 Power on the Subscriber.
This begins the installation based on the information in the .flp file. The installation begins automatically and runs with no interaction from you. After an hour or more, a message appears indicating a successful installation.

Step 2 Click the **Console** tab for the VM. Log in to the CUCM Secondary machine, using the credentials for the Administration User. The machine opens to the CLI interface.

Step 3 Right-click the VM and choose **Edit settings** and uncheck **Connect at Power on** for the floppy drive.

Create Customer Instance for 12000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 12000 agent for Cisco HCS for CC. After each task, return to this page to mark the task "done" and continue the sequence.

Table 12: Create customer instance for 12000 agent deployment of Cisco HCS for CC

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 2	
2	Set Up Virtual Machine Startup and Shutdown, on page 2	
3	Create a Domain Controller Server, on page 3	
4	Configure Unified CCE Logger , on page 96	
5	Configure Unified CCE Router, on page 98	
6	Configure Unified CCE AW-HDS, on page 98	
7	Configure Unified CCE HDS-DDS, on page 100	
8	Configure Unified CCE PG, on page 22	
9	Configure Unified CVP, on page 34	
10	Configure Cisco IOS Enterprise Voice Gateway, on page 52	
11	Configure Unified Communications Manager, on page 58	
12	Configure Unified Intelligence Center , on page 93	
13	Configure Live Data Reporting System, on page 102	
14	Configure Cisco Finesse, on page 79	
15	Single Sign-on Administration	
16	Configure Cisco Identity Service, on page 94	

Configure Unified CCE Logger

This section explains the configuration procedures you must perform for the Unified CCE Logger.

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Verify the Machine in Domain, on page 9	
3	Configure the Domain Manager, on page 10	
4	Configure Unified CCE Encryption Utility, on page 11	
5	Configure SQL Server for CCE Components, on page 11	

Sequence	Task	Done?
6	Allocate a Second Virtual Hard Drive, on page 12	
7	Configure the Unified CCE Logger, on page 12	
8	Load Base Configuration, on page 97	
9	Verify Cisco Diagnostic Framework Portico, on page 31	
10	Cisco SNMP Setup, on page 31	

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_11.6.1-Day1_12000.zip or file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Logger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Logger on Side A.

Step 5 Select the Unified CCE Logger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Logger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCE Logger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Logger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Configure Unified CCE Router

This section explains the configuration procedures you must perform for the Unified CCE Router.

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Validate Network Card, on page 35	
3	Configure Unified CCE Encryption Utility, on page 11	
4	Configure the Unified CCE Router, on page 15	
5	Verify Cisco Diagnostic Framework Portico, on page 31	
6	Cisco SNMP Setup, on page 31	

Configure Unified CCE AW-HDS

This section explains the configuration procedures you must perform for the Unified CCE AW-HDS for Sides A and B.

Table 13: Configuring Unified CCE AW-HDS for Side A and Side B

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Verify the Machine in Domain, on page 9	
3	Configure Unified CCE Encryption Utility, on page 11	
4	Configure SQL Server for CCE Components, on page 11	
5	Allocate a Second Virtual Hard Drive, on page 12	
6	AW-HDS, on page 98	
7	Verify Cisco Diagnostic Framework Portico, on page 31	
8	Cisco SNMP Setup, on page 31	
9	Set the HCS for CC Deployment Type, on page 20	

AW-HDS

- Create Instance, on page 17
- Create HDS Database, on page 18
- Configure AW-HDS, on page 99
- Database and Log File Size, on page 20

Configure AW-HDS

Complete the following procedure to install the Unified CCE Administration Server & Real-time, Historical Data Server (AW-HDS).

Procedure

Step 1 Choose **Component Management**>**Administration & Data Servers**.

Step 2 Click **Add**.

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

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

a) Click **Enterprise**.
b) Click **Large** deployment size.
c) Click **Next**.

Step 5 On the **Server Role in Large Deployment** window, configure as follows:

a) Choose the option **Administration Server and Real-time and Historical Data Server (AW-HDS)**.
b) Click **Next**.

Step 6 On the **Administration & Data Servers Connectivity** window, configure as follows:

a) Select **Primary Administration & Data Server**.
b) Enter the hostname of the secondary AW-HDS in the **Secondary Administration & Data Server** field.
c) Enter the site name in **Primary/Secondary Pair (Site) Name** field.

Note Ensure that the site name match with the site name defined under **PG Explorer** > **Agent Peripheral** > **Agent Distribution** .

d) Click **Next**.

Step 7 On the **Database and Options** window, configure as follows:

a) In the **Create Database(s)** on Drive field, select the secondary drive (typically **D** or **E**).
b) Check the **Configuration Management Service (CMS) Node**.
c) Check **Internet Script Editor (ISE) Server**.
d) Click **Next**.

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

a) For Router Side A enter the host name/IP address machine where Router A resides.
b) For Router Side B enter the host name/IP address machine where Router B resides.
c) For Logger Side A enter the host name/IP address machine where Logger A resides.
d) For Logger Side B enter the host name/IP address machine where Logger B resides.
e) Enter the **Central Controller Domain Name** .
f) Click **Central Controller Side A Preferred** .
g) Click **Next** .

Step 9 Review the **Summary** window, and click **Finish**.

Note Do not start services until all Unified CCE components are installed.

Configure Unified CCE HDS-DDS

This section explains the configuration procedures you must perform for the Unified CCE HDS-DDS for Sides A and B.

Table 14: Configuring Unified CCE HDS-DDS for Side A and Side B

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Validate Network Card, on page 35	
3	Configure Unified CCE Encryption Utility, on page 11	
4	Configure SQL Server for CCE Components, on page 11	
5	Allocate a Second Virtual Hard Drive, on page 12	
6	HDS-DDS, on page 100	
7	Verify Cisco Diagnostic Framework Portico, on page 31	
8	Cisco SNMP Setup, on page 31	

HDS-DDS

- Create Instance, on page 17
- Create HDS Database, on page 18
- Configure HDS-DDS, on page 100
- Database and Log File Size, on page 20

Configure HDS-DDS

Complete the following procedure to install the Cisco Unified CCE Administration Server & Real-time, Historical Data Server (AW-HDS).

Procedure

Step 1 Choose **Component Management**>**Administration & Data Servers**.

Step 2 Click **Add**.

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

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

a) Click **Enterprise**.
b) Click **Large** deployment size.
c) Click **Next**.

Step 5 On the **Server Role in Large Deployment** window, configure as follows:

a) Choose the option **Historical Data Server and Detailed Data Server (HDS-DDS)**.

b) Click **Next**.

Step 6 On the **Administration & Data Servers Connectivity** window, configure as follows:

a) Select **Primary Administration & Data Server**.

b) Enter the hostname of the secondary HDS-DDS in the **Secondary Administration & Data Server** field.

c) Enter the site name in **Primary/Secondary Pair (Site) Name** field.

Note Ensure that the site name match with the site name defined under **PG Explorer** > **Agent Peripheral** > **Agent Distribution** .

d) Click **Next**.

Step 7 On the **Database and Options** window, configure **Create Database(s)** on **Drive** field, select the secondary drive (typically **D** or **E**).

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

a) For Router Side A enter the host name/IP address machine where Router A resides.

b) For Router Side B enter the host name/IP address machine where Router B resides.

c) For Logger Side A enter the host name/IP address machine where Logger A resides.

d) For Logger Side B enter the host name/IP address machine where Logger B resides.

e) Enter the **Central Controller Domain Name** .

f) Click **Central Controller Side A Preferred** .

g) Click **Next** .

Step 9 Review the **Summary** window, and click **Finish**.

Note Do not service until all Unified CCE components are installed.

Configure Unified Intelligence Center

Follow these tasks to configure Unified Intelligence Center.

Sequence	Task	Done?
1	Configure Unified Intelligence Center Publisher, on page 65	
2	Configure Unified Intelligence Center Subscriber, on page 66	
3	Install VMware Tools for Windows, on page 68	
4	Configure Unified Intelligence Center Reporting, on page 68	
5	Configure Unified Intelligence Center Administration, on page 71	
6	Configure SNMP, on page 90	

Configure Live Data Reporting System

Sequence	Task	Done?
1	Configure Live Data AW-Access, on page 73	
2	Configure Live Data Machine Services, on page 74	
3	Configure Live Data Unified Intelligence Data Sources, on page 75	
4	Configure Live Data Reporting Interval, on page 76	
5	Import Reports, on page 41	
6	Add Certificate for HTTPS Gadget, on page 78	

Create Customer Instance for 24000 Agent Deployment Model

Follow this sequence of tasks to create the customer instance to deploy 24000 agent for Cisco HCS for CC. After each task, return to this page to mark the task "done" and continue the sequence.

Table 15: Create customer instance for 24000 agent deployment of Cisco HCS for CC

Sequence	Task	Done?
1	Upgrade VMware Tools, on page 2	
2	Set Up Virtual Machine Startup and Shutdown, on page 2	
3	Create a Domain Controller Server, on page 3	
4	Configure Unified CCE Logger , on page 96	
5	Configure Unified CCE Router, on page 98	
6	Configure Unified CCE AW-HDS, on page 98	
7	Configure Unified CCE HDS-DDS, on page 100	
8	Configure Unified CCE PG, on page 22	
9	Configure Unified CVP, on page 34	
11	Configure Cisco IOS Enterprise Voice Gateway, on page 52	
12	Configure Unified Communications Manager, on page 58	
13	Configure Unified Intelligence Center , on page 93	
14	Configure Live Data Reporting System, on page 102	
15	Configure Cisco Finesse, on page 79	

Sequence	Task	Done?
16	Single Sign-on Administration	
17	Configure Cisco Identity Service, on page 94	

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Based on your timezone, download the HCS-CC_12.0.1-Day1_24000.zip or file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Logger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Logger on Side A.

Step 5 Select the Unified CCE Logger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Logger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCE Logger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Logger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Create Customer Instance for Small Contact Center Agent Deployment Model

Follow these sequence of tasks to create the customer instance to deploy small agent for Cisco HCS for CC for Contact Center. After each task, return to this page and mark the task “done” and continue the sequence.

Table 16: Create Customer Instance for core components

Sequence	Task	Done
1	Upgrade VMware Tools, on page 2	
2	Set Up Virtual Machine Startup and Shutdown, on page 2	
3	Create DNS Server for Finesse in Small Contact Center Deployment, on page 107	
4	Configure Unified CCE Rogger for Small Contact Center Agent Deployment , on page 105	
5	Configure Unified CCE AW-HDS-DDS, on page 16	
6	Configure VRU Peripheral Gateway, on page 25	
7	Configure Unified CVP, on page 34	
8	Configure CUBE Enterprise for Small Contact Center Deployment Model, on page 111	
9	Configure Unified Intelligence Center , on page 93	
10	Configure Live Data Reporting System, on page 93	

Table 17: Configure Dedicated Components Sub Customer Option

Sequence	Task	Done
1	Set Up Virtual Machine Startup and Shutdown, on page 2	
2	Configure Unified CCE PG, on page 22	
3	Configure Unified Communications Manager, on page 58	
4	Increase the SW MTP and SW Conference Resources	
5	Configure Cisco Finesse, on page 79	
6	Configure Cisco Identity Service, on page 94	

Table 18: Configure Shared Components Sub Customer Option

Sequence	Task	Done
1	Set Up Virtual Machine Startup and Shutdown, on page 2	
2	Configure Unified CCE PG, on page 22	
3	Configure Shared Unified Communications Manager, on page 107	
4	Configure Cisco Finesse, on page 79	
5	Configure Cisco Identity Service, on page 94	

After creating customer instance for shared core components and sub customer components for small contact center agent deployment, configure unified CCDM to integrate with the Internet Script Editor. See Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM

After creating customer instance for shared core components and sub customer components for small contact center agent deployment:

- Configure unified CCDM to integrate with the Internet Script Editor. See Integration of Small Contact Center Agent Deployment for Partition Internet Script Editor with CCDM.
-

Configure Unified CCE Rogger for Small Contact Center Agent Deployment

This section explains the configuration procedures you must perform for the Unified CCE Rogger.

Sequence	Task	Done?
1	Configure Network Cards, on page 7	
2	Verify the Machine in Domain, on page 9	
3	Configure the Domain Manager, on page 10	
4	Configure Unified CCE Encryption Utility, on page 11	
5	Configure SQL Server for CCE Components, on page 11	
6	Allocate a Second Virtual Hard Drive, on page 12	
7	Configure the Unified CCE Logger, on page 12	
8	Configure Unified CCE Router for Small Contact Center, on page 106	
9	Load Base Configuration, on page 105	
10	Verify Cisco Diagnostic Framework Portico, on page 31	
11	Cisco SNMP Setup, on page 31	

Load Base Configuration

Complete this procedure to import base configuration parameters.

Procedure

Step 1 Download the HCS-CC_11.6.1-Day1_SCC.zip or file. Save it locally and unzip it.

Step 2 Download the Domain_Update_Tool.zip file. Save it locally and unzip it.

Step 3 Copy the configuration folder to the local drive of Unified CCE Rogger on Side A.

Step 4 Open the ICMDBA Tool on the Unified CCE Rogger on Side A.

Step 5 Select the Unified CCE Rogger and expand the tree to <instance name>_sideA.

Step 6 Select Data on the menu bar and click **Import**.

Step 7 Browse to locate the configuration folder and click **Open**.

Step 8 Click **OK** and then click **Import**.

Step 9 Click Start and then click **OK** on all messages.

Step 10 Navigate to the folder Domain_Update_Tool and right-click UpdateDomain.PS1. and Run with PowerShell. Respond as follows:

a) For Server name, enter the computer name of the Unified CCE Rogger Side A.
b) For Database name, enter <instance_sideA (Logger database)>.
c) For Domain Name, enter the customer's domain name.

Step 11 Return to the ICMDBA tool. Select Logger <instance name> database for the side that you want to synchronize.

Step 12 Click **Data** in menu bar and select **Synchronize** and perform the following:

a) In **Synchronize** window, click **Add** in **Source** pane.
b) Enter hostname for Unified CCE Rogger of source in **Server Name** field and click **OK**.
c) Click **Add** in **Destination** pane.
d) Enter hostname for Unified CCE Rogger of destination in **Server Name** field and click **OK**.
e) Click **Synchronize**.

Step 13 Click **Start** and then click **OK** on all messages.

Configure Unified CCE Router for Small Contact Center

Complete the following procedure to configure the Unified CCE Router.

Procedure

Step 1 Launch the Unified CCE Web Setup.

Step 2 Sign in as the domain user with local Administrator permission.

Step 3 Navigate to **Component Management** > **Routers**.

Step 4 Click **Add** to set up the Call Router.

Step 5 In the Deployment window, select the appropriate **Side**.

Step 6 Select **Duplexed** and click **Next**.

Step 7 In the **Router Connectivity** window, configure the Private Interface and Public (Visible) Interfaces. Click **Next**.

Step 8 In the **Enable Peripheral Gateways** field, enter the number assigned to the PGs to enable it.

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

Note Enter only the IDs of the PGs which exist in the system. Adding unused PG IDs can cause incorrect Router failover handling.

Step 9 For PGs 81-150, click **Advanced** to expand it and enter the PG numbers to be used.

Step 10 In the **Router Options** window, configure the following, and click **Next** .

a) Check **Enable Database Routing**
b) Check **Enable Quality of Service (QoS)**. (Applicable to Side A only.)

Step 11 In **Router Quality of Service** window, click **Next** .

Step 12 In the **Summary** window, make sure that the Router summary is correct, then click **Finish** .

Note Do not start service until all Unified CCE components are installed.

Configure Shared Unified Communications Manager

Follow this sequence of tasks to configure shared Unified Communications Manager:

Sequence	Task	Done?
1	Configure Unified Communications Manager Publisher, on page 58	
2	Configure Unified Communications Manager Subscriber, on page 59	
3	Install VMware Tools for Windows, on page 68	
4	Unified Communications Manager License, on page 60	
5	Activate Services , on page 61	
6	Validate Clusterwide Domain Configuration, on page 62	
7	Upgrade Cisco JTAPI Client on PG, on page 30	
8	Configure SNMP, on page 90	
9	Setup Partition	
10	Setup Calling Search Space	
11	Associate CSS and Partition with Phones and Lines	
12	Associate CSS with Trunk	

Create DNS Server for Finesse in Small Contact Center Deployment

Few VOS machines (like Finesse) require a DNS server resolution to be locally available in the same network for successful VOS installation. Install DNS in the Sub customer network for Small Contact Center deployment.

Complete the following procedures to create DNS server:

- Enable DNS Server, on page 5
- Configure DNS Server, on page 109

Enable DNS Server

Procedure

Step 1 Go to **Start** > **Server Manager**.

Step 2 In the **Server Manager** window, select **Manage** > **Add Roles and Features**.

Step 3 In the **Before You Begin** tab, click **Next**.

Step 4 In the **Installation Type** tab, choose **Role based or feature based installation** option and click **Next**.

Step 5 The **Server Selection** tab, displays the list of servers that are running on Windows Server. Select a server from this list and click **Next**.

Step 6 On the **Server Roles** tab, do the following:

a) Select the **Active Directory Domain Services** if you intend to promote a domain controller.

b) In the **Add Features that are required for Active Directory Domain Services?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools
    - AD DS and AS LS Tools
      - [Tools] AS DS Snap-Ins and Command-Line Tools
      - [Tools] Active Directory Administrative Center

Step 7 Select **DNS Server**.

Step 8 In the **Add Features that are required for DNS Server?** dialog box, ensure the following tools are listed and then click **Add Features**.

- Remote Server Administration Tools
  - Role Administration Tools
    - [Tools] DNS Server Tools

Step 9 In the **Features** tab, ensure **Remote Server Administration Tools and Role Administration Tools** are selected and click **Next**.

Step 10 In the **AD DS** tab, click Next.

Step 11 In the **DNS Sever** tab, click Next.

Step 12 n the **Confirmation** tab, click Install.
The **Result** tab displays the progress of the DNS server installation.

Step 13 After the installation completes, click on the **Promote this server to a domain controller** link to make the server a domain controller.

Step 14 In the **Deployment Configuration** tab, select **Add a New Forest,** enter a valid fully qualified domain DNS name, and click **Next**.

Note Enter a valid domain name that adheres to the naming conventions listed at https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

Step 15 In the **Domain Controller Options** tab, enter the following and click **Next**:

a) From the **Forest functional level** drop-down list, select Windows Server version based on your AD version.

b) From the **Domain functional level** drop-down list, select Windows Server version based on your AD version.

Note You can also choose to set the forest functional level to an older Windows Server version.

However, the Windows Server 2012 forest functional level does not provide any new functionality over the Windows Server 2008 R2 forest functional level.

c) Ensure that the **Domain Name System (DNS) Server** and the **Global Catalog (GC)** check box is checked.

d) Set the **Directory Services Restore Mode** password.

Step 16 In the **Additional Options** tab, enter the **NetBios** name and click **Next**.

Step 17 In the **Paths** tab, enter the paths where you would like to store the database, log files, and SYSVOL.

Step 18 In the **Review Options** tab, click **Next**.

Step 19 In the **Prerequisites Check** tab, you can read through the warning if any and click **Install**.
The **Results** page displays whether the installation was a success. The server will automatically reboot in 10 minutes.

Configure DNS Server

Procedure

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

Step 2 Expand the **Server** on Left side pane.

Step 3 Right-click on Forward Lookup Zones and Click **New Zone**.

Step 4 In the New Zone Wizard, Click **Next**.

Step 5 In the Zone type window, choose **Primary zone**. Click **Next**.

Step 6 In the Zone Name window, Enter the *Fully qualified DNS name*. Click **Next**.

Step 7 In Zone File window, Choose **Create a new file with this file name**. Click **Next**.

Step 8 In the Dynamic Update window, Choose **Do not allow dynamic updates**. Click **Next**

Step 9 Click **Finish**.

Step 10 Right-click on Reverse Lookup Zones and Click **New zone**.

Step 11 In the New Zone Wizard, Click **Next**

Step 12 In the Zone type window, choose **Primary zone**. Click **Next**.

Step 13 In the Reverse Lookup Zone Name, choose **IPv4 Reverse Lookup Zone**. Click **Next**.

Step 14 Enter the *first three octets of IP address* in **Network** field. Click **Next**.

Note For Small Contact Center deployment model customer needs to add reverse lookup zone for both shared and Internal IP's, only if customer is using shared DNS for finesse Installation.

Example:

Create Reverse Lookup zone for 10.10.10.X (Shared IP) and 20.20.20.X (Internal IP).

Step 15 In Zone File window, Choose **Create a new file with this file name**. Click **Next**.

Step 16 In the Dynamic Update window, Choose **Do not allow dynamic updates**. Click **Next**.

Step 17 Click **Finish**.

Configure Host in DNS Server

Procedure

Step 1 Navigate to **DNS Manager**.

Step 2 Right click on the **Forward domain zone**. Select **New Host (A or AAAA)**.

Step 3 Enter Host Name.

Step 4 Enter IP address of the host.

Step 5 Check the **Create associated pointer (PTR) Record** check box. Click **Add host**.

Step 6 Click **Ok**. Click **Done**

Note For Small Contact Center Deployment model, if the customer is using shared DNS for finesse installation perform the following steps:

a. Add finesse internal IP (not the natted IP) in both Forward and Reverse lookup zone of shared DNS.

b. Add the unique finesse hostname in DNS server where ip address can be same.

c. After successfull installation of finesse primary and secondary, remove the host entry from Reverse look up zone of finesse internal IP.

d. Add the natted IP for finesse hostname in the DNS server, this supports SSO.

Note Live Data is not supported with shared DNS configuration for dedicated sub-customer option.

e. The OS customization of Finesse servers for all sub customers should be done in sequential manner not in parallel.

Configure CUBE Enterprise for Small Contact Center Deployment Model

Configure VRF

The Multi-VRF feature allows you to configure and maintain more than one instance of routing and forwarding tables within the same CUBE device and segregate voice traffic based on the VRF.

Configure VRF for Sub-customer 1:

```
ip vrf SUB-Customer1
rd 20.20.20.10:1
```

This creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y)

Configure VRF for Sub-customer 2:

```
ip vrf SUB-Customer2
rd 20.20.20.10:2
```

Assign Interface to VRF

To assign an interface to the VRF, perform the following instructions :

```
interface GigabitEthernet2
 ip vrf forwarding Customer1
```

Associates the VRF with the interface. If there is an IP address associated with the interface, it will be cleared and you will be prompted to assign the IP address again.

```
 ip address 10.10.10.5 255.255.255.0
```

Configure Global Settings

```
 voice service voip
 no ip address trusted authenticate
 address-hiding
 mode border-element
```

Configure Codec List

```
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
codec preference 3 g729br8
codec preference 5 g711alaw
```

Configure Default Services

```
Default Services
application
service survivability flash:survivability.tcl
```

Configure VRF Specific RTP Port Ranges

For VoIP RTP connections, you can configure each VRF to have its own set of RTP port range under voice service VoIP. A maximum of ten VRF port ranges are supported. Different VRFs can have overlapping RTP port range.

The VRF based RTP port range limits, including the minimum and maximum port numbers, are the same as the global RTP port range. All the three port ranges, global, media-address, and VRF based can coexist on CUBE. The preference order of the RTP port allocation is as follows:

- VRF based port range
- Media-address based port range
- Global RTP port range

```
media-address voice-vrf SUB-Customer1 port-range 25000 28000
media-address voice-vrf SUB-Customer2 port-range 25000 28000
```

Configure IP Route

```
ip route vrf SUB-Customer1 0.0.0.0 0.0.0.0 20.20.20.1
ip route vrf SUB-Customer2 0.0.0.0 0.0.0.0 20.20.20.1
```

Configure Dial Peer

Control and media on a dial-peer have to bind with same VRF. Else, while configuring, the CLI parser will display an error.

Configure Incoming Dial Peer for CVP

```
dial-peer voice 23991 voip
 description Incoming dial-peer for CVP
 service survivability
 session protocol sipv2
 session transport udp
 incoming called-number .T
 voice-class codec 1
 voice-class sip rel1xx disable
 voice-class sip bind control source-interface GigabitEthernet1
 voice-class sip bind media source-interface GigabitEthernet1
 dtmf-relay rtp-nte
```

Configure Outbound Dial Peer for CVP

```
dial-peer voice 1001 voip
description outgoing dial-peer for CVP
translation-profile outgoing strip-digit
destination-pattern .T
session protocol sipv2
session target ipv4:10.10.10.10
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet1
voice-class sip bind media source-interface GigabitEthernet1
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Configure Incoming Dial Peer for Sub-customer1 VRF1

```
dial-peer voice 21991 voip
description "Incoming Dial-peer for VRF1"
service survivability
session protocol sipv2
session transport udp
incoming called-number [12][03][27].......
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte
```

Incoming Dial Peer for Sub-customer2 VRF2

```
dial-peer voice 22991 voip
description "Incoming dial-peer for VRF2"
service survivability
session protocol sipv2
session transport udp
incoming called-number 1[03][16].......
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet3
voice-class sip bind media source-interface GigabitEthernet3
dtmf-relay rtp-nte
```

Configure Dial-Peer for Sub-customer1 VRF1

```
dial-peer voice 21001 voip
description from CVP towards VRF1 to CUCM Sub-Customer1
destination-pattern 101....
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.100
voice-class sip bind media source-interface GigabitEthernet2.100
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

Configure Dial-Peer for Sub-customer2 VRF2

```
dial-peer voice 22001 voip
description from CVP towards VRF2 to CUCM Sub-Customer2
destination-pattern 201....
session protocol sipv2
session target ipv4:20.20.20.31
session transport udp
voice-class codec 1
voice-class sip rel1xx disable
voice-class sip bind control source-interface GigabitEthernet2.200
voice-class sip bind media source-interface GigabitEthernet2.200
dtmf-relay rtp-nte h245-signal h245-alphanumeric
```