Installation

Installation Task Flow

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

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

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

Task	See
Ensure that virtual machines are ready for installation	Set Up Virtual Machines for Installation
Install Unified Communications Manager	Installing Cisco Unified Communications Manager
Install Unified CCE components (Router, Logger, Administration & Data Servers, peripherals)	Install Unified CCE Software, on page 3
Install Outbound Option	Create Outbound Option Database, on page 8 and then see *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html
Install Finesse	Cisco Finesse Server Installation, on page 33
Install Enterprise Chat and Email	Enterprise Chat and Email Installation Guide (for Unified Contact Center Enterprise) at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html

Task	See
Install Single Sign-On Identity Service Standalone (4000, 8000, 12000 Agent Deployment) or Install Coresident Deployment (2000 Agent Deployment)	Install Cisco Identity Service Standalone Deployment, on page 45 or Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 54
Install Cisco Unified Intelligence Center Standalone (4000, 8000, 12000 Agent Deployment) or Install Coresident Deployment (2000 Agent Deployment)	*Installation and Upgrade Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-installation-guides-list.html or Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 54
Install Live Data Standalone (4000, 8000, 12000 Agent Deployment) or Install Coresident Deployment (2000 Agent Deployment)	Live Data Standalone Installation, on page 49 or Install Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 54
Install Cisco Unified Customer Voice Portal (Unified CVP) [1]	*Installation and Upgrade Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-guides-list.html
Install Unified Contact Center Management Portal (Unified CCMP)	*Installation and Configuration Guide for Cisco Unified Contact Center Management Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-management-portal/products-installation-guides-list.html
Install Cloud Connect (2000 Agent Deployment)	Install Cloud Connect, on page 59

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

Installation Tasks

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

Note Take a backup of the VM snapshot before installing the Unified CCE software, because uninstallation support is not provided for 12.5(1) .

Note Uninstallation is supported for Unified CCE 12.6(x). Uninstalling Unified CCE 12.6(x) brings the component back to the previous version.

Install Unified CCE Software

Before you begin

Before installing Unified CCE 12.6(2), you must install Unified CCE 12.5(1). While installing Unified CCE 12.5(1), you can perform an in-line upgrade to Unified CCE 12.6(2).

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

Note During Unified CCE installation on Windows Server 2019 and SQL Server 2019, do not select the SQL Server Security Hardening optional configuration as part of installation. Post the installation of Unified CCE 12.6(2), use the Security Wizard tool to apply SQL Security Hardening.

Procedure

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

Step 2 Open the ICM-CCE-Installer, click **Next**.

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

Step 4 To apply Unified ICM Maintenance 12.6(2) Release, click **Browse** and navigate to the Maintenance Release software.

Note You can also proceed with the installation of Unified ICM 12.5(1) without selecting Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 8.

Step 5 The installer program proceeds through a series of screens on which you specify information.

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

Step 6 Select **Yes** for the system to restart and complete the installation automatically or select **No** to restart the system manually after installing Unified ICM 12.5(1).

Note
- If you have selected Unified ICM 12.6(2) in step 4, you must select **Yes** for the system to restart automatically.
- After installing Unified ICM 12.5(1), you must restart the system manually before launching the Unified ICM 12.6(2) installation wizard and proceeding to step 8.

Step 7 Log in to your system using domain credentials with administrative privileges.

Step 8 Wait for the Unified CCE 12.6(2) installation wizard to launch. Click **Next** to proceed.

Step 9 Select the radio button to accept the license agreement and click **Next**.

Step 10 Click **Install** to begin the installation.

Step 11 Select the radio button to restart the system and click **Finish**.

Set up Organizational Units

Add a Domain

Use the Domain Manager tool to add a domain.

Procedure

Step 1 Log in with a Domain Administrator privilege.

Step 2 Open the **Domain Manager** Tool from Unified CCE Tools shortcut on your desktop.

Step 3 Click **Select**. under **Domains**.

Step 4 You can add domains through the **Select Domains** dialog box, or you can add a domain manually if the target domain cannot be detected automatically.

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

a) In the left pane under Choose domains, select one or more domains.
b) Click **Add** to add the selected domains, or click **Add All** to add all the domains.

To add a domain manually:

a) In the field under Enter domain name, enter the fully qualified domain name to add.
b) Click **Add**.
c) Click **OK**.

Add Organizational Units

Use the Domain Manager tool to create the Cisco root Organizational Unit (OU) for a domain, and then create the facility and instance OUs.

The system software always uses the root OU named Cisco_ICM. You can place the Cisco_ICM OU at any level within the domain where the Unified ICM Central Controller is installed. The system software components locate the root OU by searching for this name.

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

Procedure

Step 1 Log in with a domain administrator privilege and open the **Domain Manager** Tool from Unified CCE Tools shortcut on the desktop.

Step 2 Choose the domain.

Step 3 If this OU is the first instance, then perform the following steps to add the Cisco_ICM root:

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

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

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

Step 4 Add the facility OU:

a) Select the Cisco Root OU under which you want to create the facility OU.

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

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

Step 5 Add the instance OU:

a) Navigate to and select the facility OU under which you want to create the instance OU.

b) In the right pane, under Instance, click **Add**.

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

Step 6 Click **Close**.

Add Users to Security Groups

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

Procedure

Step 1 Open the Domain Manager tool and select the Security Group (**Config** or **Setup**) you want to add a user to.

Step 2 Under Security group, click **Members**.

Step 3 Under Users, click **Add**.

Step 4 Select the domain of the user you want to add.

Step 5 (Optional) In the **Optional Filter** field, choose to further filter by the Name or User Logon Name, apply the search condition, and enter the search value.

Step 6 Click **Search**.

Step 7 Select the member you want to add to the Security Group from the search results.

Step 8 Click **OK**.

Add Unified CCE Instance

Procedure

Step 1 Open the Unified CCE Web Setup tool from shortcut on your desktop.

Step 2 Sign in as a domain user with local administrator rights.

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

Step 4 On the **Add Instance** page, from the drop-down list, choose the customer **Facility and Instance**.

Step 5 Enter an instance number.

The same instance name can occur more than once in a domain, so the instance number provides the uniqueness. The instance number must be between 0 and 24. The instance number must match for the same instance across your entire deployment. For an Enterprise (single instance) deployment, select 0 unless there are reasons to select another value.

Step 6 Click **Save**.

Note These steps of adding instance must be repeated on each Windows Server VM that hosts the Unified ICM component(s).

Set Up Unified CCE Central Controller and Administration and Data Server Components

Create Component Databases

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

Create Logger Database

Perform this procedure on the Side A and Side B Logger/Rogger VM.

Procedure

Step 1 From Unified CCE Tools, open the ICMDBA tool, and click **Yes** at any warnings that display.

Step 2 Navigate to **Server** > **Instances**.

Step 3 Right-click the instance name and choose **Create** to create the logger database.

Step 4 In the Select Component dialog box, choose the logger you are working on (Logger A or Logger B). Click **OK**.

Step 5 At the prompt, “SQL Server is not configured properly. Do you want to configure it now?”, click **Yes**.

Step 6 On the Configure page, in the SQL Server Configurations pane check **Memory (MB) and Recovery Interval**. Click **OK**.

Step 7 On the Stop Server page, click **Yes** to stop the services.

Step 8 In the Select Logger Type dialog box, choose **Enterprise**. Click **OK** to open the Create Database dialog box.

Step 9 Create the Logger database and log as follows:

a) In the DB Type field, choose the Side (A or B).
b) In the region field, choose your region.
c) In the Create Database dialog box, click **Add** to open the Add Device dialog box.
d) Click **Data**.
e) Choose the drive on which you want to create the database, for example, the E drive.
f) For the **Size** field, consider whether to choose the default (which is 1.4GB, a fairly minimal size) or calculate a value appropriate for your deployment by using the Database Size Estimator Tool. If you calculate the value, enter it here.

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

a) Click **OK** to return to the Create Database dialog box.
b) Click **Add** again.
c) In the Add Device dialog box, click **Log**.
d) Choose the drive where you created the database.
e) In the **Size** field, choose the default setting or, if you have calculated an appropriate size for your deployment, enter that value.
f) Click **OK** to return to the Create Database dialog box.

Step 10 In the Create Database dialog box, click **Create**, then click **Start**.

Step 11 When you see the successful creation message, click **OK** and then **Close**.

Create HDS Database

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

Procedure

Step 1 Open the ICMDBA tool, and click **Yes** at any warnings that display.

Step 2 Navigate to **Servers** > **Instances**.

Step 3 Right-click the instance name and choose **Create**.

Step 4 In the Select Component dialog box, choose **Administration & Data Server**. Click **OK**.

Step 5 At the prompt “SQL Server is not configured properly. Do you want to configure it now?”, click **Yes**.

Step 6 On the Configure dialog box, click **OK**.

Step 7 On the Select AW Type dialog box, choose **Enterprise**. Click **OK** to open the Create Database dialog box.

Step 8 Create the HDS database as follows:

a) From the DB Type drop-down list, choose **HDS**.
b) Click **Add**.
c) On the Add Device dialog box, select **Data**.

d) From the Available Drives list, choose the drive on which you want to install the database.
e) In the Size field, you can leave the default value or enter an appropriate size for your deployment.

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

Note You can use the Database Size Estimator Tool to calculate the appropriate size for your deployment.

f) Click **OK** to return to the Create Database dialog box.
g) Click **Add**.
h) On the Add Device dialog box, select **Log**.
i) From the Available Drives list, choose the drive on which you created the database.
j) In the Size field, you can leave the default value or enter an appropriate size for your deployment.
k) Click **OK** to return to the Create Database dialog box.

Step 9 On the Create Database dialog box, click **Create** and then click **Start**.

Step 10 When you see the successful creation message, click **OK** and then click **Close**.

Create Outbound Option Database

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

After you complete this procedure, see the *Outbound Option Guide for Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-user-guide-list.html .

Procedure

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

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

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

Step 4 In the Create Database dialog box, click **Add** to open the Add Device dialog box.

Step 5 Click **Data**, and choose the drive on which you want to create the database, for example, the E drive. In the database size field, you can choose to retain the default value or enter a required value.

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

Step 6 Click **OK** to return to the Create Database dialog box.

Step 7 In the Add Device dialog box, click **Log**. Choose the desired drive. Retain the default value in the log size field and click **OK** to return to the Create Database dialog box.

Step 8 In the Create Database dialog box, click **Create**, and then click **Start**. When you see the successful creation message, click **OK** and then click **Close**.

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

Add Components to Unified CCE Instance

Add Logger Component to Instance

Perform this procedure on the Side A and Side B Loggers; both logger machines must be up and operational.

Before you begin

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

Procedure

Step 1 Open the Web Setup tool.

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

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

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

Step 5 If an external AW-HDS-DDS exists in the deployment, check **Enable Historical/Detail Data Replication**. If no external AW-HDS-DDS exists in the deployment, leave **Enable Historical/Detail Data Replication** unchecked.

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

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

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

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

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

Note Disabling HA will not disable outbound option, customer has to explicitly disable outbound when HA is disabled.

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

Step 10 If you enable High Availability, enter the **Active Directory Account Name** that the opposite side logger runs under or a security group that includes that account. For example, if you are running Websetup on the logger on Side A, enter the name of the Active Directory account (or security group) that is run on Side B logger.

Step 11 Select the **Syslog** box to enable the Syslog event feed process (cw2kfeed.exe).

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

Step 12 Click **Next**.

Step 13 On the Data Retention page, modify the Database Retention Configuration table:

a) For these tables, set the retention period to 40 days:

- Application_Event
- Event
- Network_Event
- Route_Call_Detail
- Route_Call_Variable
- Termination_Call_Detail
- Termination_Call_Variable

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

Step 14 Click **Next**.

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

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

Step 17 Click **Next**.

Add Router Component to Instance

Perform this procedure for Side A and Side B Routers.

Procedure

Step 1 In the Web Setup tool, select **Component Management** > **Routers**.

Step 2 Click **Add** to set up the Call Router.

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

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

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

Step 6 In the **Router Connectivity** dialog, configure the Private Interface and Public Interfaces. Click **Next**.

Note For the address input fields, use Fully Qualified Domain Names instead of IP addresses.

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

Step 7 In the **Enable Peripheral Gateways** field, enter the number assigned to the PGs to enable it. Click **Next**.

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

Step 8 In the **Router Options** dialog, the **Enable Quality of Service (QoS)** is enabled by default. Click **Next**.

On the Router Quality of Service page, you see preconfigured values for the Router QoS for the Private Network. These values only appear if you selected a Side A Router. You can change the values in the DSCP fields if necessary.

Keep QoS enabled for all Unified CCE Private network traffic. For most deployments, disable QoS for the public network traffic. For more details, refer to the appropriate section in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Step 9 In the **Router Quality of Service** dialog, click **Next**.

Step 10 In the **Summary** dialog, make sure that the Router summary is correct, then click **Finish**.

Add Administration & Data Server Component to Instance

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

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

Not all fields apply to all server types.

Note AW Database is created when you add **Administration & Data Server** Component. Data from the **Config_Message_Log table** is replicated from the Logger database to the AW database; you can use the AW database for auditing purposes. When you add the Administration & Data Server component, the retention period for the Config_Message_Log table in the AW database defaults of 90 days. To change the retention period, modify the following registry key: `Cisco Systems, Inc.\ICM\<instancename>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Retain\System\ConfigMessageLog`.

Procedure

Step 1 Open the Web Setup tool.

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

Step 3 On the **Deployment** page, configure as follows:

a) Choose the current instance.

b) Choose the deployment type as **Enterprise**.

c) Choose the deployment size. If you choose **Small to Medium**, go to step 4. If you choose **Large**, go to step 5.

Note For deployment size definitions and guidelines, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise*.

d) Click **Next**.

Step 4 On the **Role** page, in the Server Role in a Small to Medium Deployment section, select the radio button for your preferred option.

The three options from which to select are:

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

Note If you select AW-HDS-DDS, you must also specify Enable Historical Detail Data Replication during Logger setup.

Note Before you select a role that includes Historical Database Server (HDS), you must deploy an HDS database on this instance by running the Cisco Unified Intelligent Contact Management Database Administration Tool (ICMDBA) on the local machine.

Step 5 On the **Role** page, in the Server Role in a Large Deployment section, select the radio button for your preferred option.

The four options from which to select are:

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

Note If you select AW-HDS or HDS-DDS, you must also specify Enable Historical Detail Data Replication during Logger setup.

Note Before you select a role that includes Historical Database Server (HDS), you must deploy an HDS database on this instance by running ICMDBA on the local machine.

Step 6 Click **Next**.

Step 7 On the **Administration & Data Server Connectivity** page, enter connectivity information between Primary and Secondary Administration and Data servers.

Note Each site has at least one and usually two Administration & Data Servers that serve as real-time data Administration & Data Servers for the site. The primary Administration & Data Server maintains an active connection to the real-time server through which it receives real-time data. If the site has two Administration & Data Servers, Administration Clients are configured to automatically switch to a secondary Administration & Data Server if the first Administration & Data Server becomes non-functional for any reason. The secondary Administration & Data Server also maintains connections to the real-time server; however, these connections remain idle until needed. The secondary Administration & Data Server uses the primary Administration & Data Server, as its source for the real-time feed.

Indicate whether the server being setup is the Primary or Secondary Administration & Data Server at the site, by clicking on the radio button.

Next enter the host name or IP address of the Primary and Secondary Administration and Data Server at the site. The Secondary Administration and Data Server field is mandatory. If there is no secondary Administration and Data Server being deployed at the site, then the same host name as that of the primary needs to be provided in this field.

Each primary and secondary pair must have its own Site Name, and the Site Name must be exactly the same on both Administration & Data Servers for them to be logically viewed as one.

Step 8 Click **Next**.

Step 9 On the **Database and Options** page, configure as follows:

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

Step 10 On the **Central Controller Connectivity** page, configure as follows:

a) For **Router Side A**, enter the Router Side A IP address.
b) For **Router Side B**, enter the Router Side B IP address.
c) For **Logger Side A**, enter the Logger Side A IP address.
d) For **Logger Side B**, enter the Logger Side B IP address.
e) Enter the **Central Controller Domain Name**.
f) Based on the Reference Design of your deployment type, distribute your AW-HDS and HDS-DDS VMs on Side A or Side B by selecting **Central Controller Side A Preferred** or **Central Controller Side B Preferred**. For details on the Reference Designs, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_5_1/design/guide/ucce_b_soldg-for-unified-cce-12_5.html .
g) Click **Next**.

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

Set up Peripheral Gateways

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

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

Configure Peripheral Gateways in PG Explorer

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

Not all fields apply to all PG types.

Before you begin

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

Procedure

Step 1 From your desktop, double-click the Unified CCE Tools icon, and open Administration Tools folder from Unified CCE Tools icon on the desktop.

Step 2 Double-click the Configuration Manager icon.

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

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

Step 5 Complete the Logical Controller section as follows:

a) **Logical Controller ID**—Leave blank. This value is generated automatically when the record is saved.
b) **Physical Controller ID**—Leave blank. This value is generated automatically when the record is saved.
c) **Name**—Enter a unique enterprise name for the PG.
d) **Client Type**—Select as follows from the drop-down list:

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

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

f) **Description**—Enter any other information about the PG. Configuration Manager copies this value to the description fields of the logical interface controller, physical interface controller, peripheral, and (if applicable) the routing client records.
g) **Physical Controller Description**—Enter a description for the physical controller.
h) **Primary CTI Address**—Enter the address for the primary CTI server. Make this entry in the form of <IP address or server name where the CTI server is installed>: <Client Connection Port Number>.
i) **Secondary CTI Address**—Enter an address for a secondary CTI server (for duplexed systems).
j) **Reporting Interval**—Select the 15 or 30 Minute reporting interval option (default is 30 Minute). Unified CCE software stores historical information in either half-hour or 15-minute summaries (but not both), based on the reporting interval value that you set. The Router sends these records to the Logger, which in turn writes them to the Central Database.

Step 6 Do not exit the PG Explorer tool. You add a peripheral to the PG and save the configuration in the next procedure.

Add Peripherals to Peripheral Gateways

Fields can vary according to PG type.

Procedure

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

Step 2 On the Peripheral tab, enter the following:

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

- For a CUCM PG: CUCM
  - Configure Agent Desk settings before adding CUCM PG. See Assign Agent Desk Settings
- For a VRU PG: VRU
  - Configure Network VRU before adding VRU PG. See Configure Network VRUs
- For an MR PG: MediaRouting
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

d) **Location**—Enter the peripheral's location, for example, the name of a city, building, or department.
e) **Abandoned Call Wait Time**—Enter the minimum time (in seconds) an incoming call must be queued before being considered an abandoned call if the caller ends the call.
f) **Configuration Parameters**—As desired, enter a string containing any parameters that must be sent to the device to initialize it. In most cases, you leave this field blank.
g) **Peripheral Service Level Type**—The default type of service level calculation that the peripheral performs for its associated services. Select **Calculated by Call Center**.

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

i) **Agent Phone Line Control**—Specify one of the following agent phone line control options:

- **Single Line:** Enables single-line monitoring and reporting (default).
- **All Lines:** Enables multiline monitoring and reporting.

j) **NonACD Line Impact**—Specify one of the following nonACD line impact options:

- **Available Agent Goes Not Ready:** Agent state is set to Not Ready with a system reason code when the agent answers or calls out on a secondary line while in the Available or Not Ready state.
- **Available Agent Stays Available:** Agent state is unchanged when agent is on a call on a secondary line.

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

l) **Default Desk Settings**—Select as follows:

- For a CUCM PG: Select the Agent Desk Settings that you created earlier
- For a VRU PG: None
- For an MR PG: None
- For a UCC Enterprise Gateway PG: None

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

Step 3 On the Advanced tab, enter the following:

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

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

c) **Network VRU**—The type of network VRU. Select as follows:

- For a CUCM PG: None
- For a VRU PG: Select the corresponding Network VRU that you created earlier.
- For an MR PG: Select the Type 2 Network VRU that you created earlier.
- For a UCC Enterprise Gateway PG: None

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

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

f) **Agent Targeting Mode**—Determines how the Router builds the labels. Select **Rule Preferred**.

When this check box is checked, only the local PG can target agents on the PG. The Router uses the skill group IPTA configuration to select agents. When this check box is unchecked, for calls routed between different PGs, the Router picks the agent (which minimizes the benefit of the Unified CCE System PG). Unchecking the check box also requires the creation of more device targets.

Step 4 On the Agent Distribution tab, enter the following:

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

b) **Agent Event Detail**—Enables label text (as opposed to numeric) Not Ready Reason Code reporting.
c) The Agent Distribution Entries section of this tab contains entries for agent Administration & Data Servers available for distributing agent report data for the selected peripheral. Click **New**, then define the values in the Currently Selected site section of this tab as follows:

- **Administration & Data Server site name:** The name of the currently selected site in the agent distribution entries list. For MR PGs, do not specify a name for this field.
- **Agent real time data:** Check to enable the flow of agent real-time data from the peripheral to the Administration & Data Server. Uncheck to disable the flow of agent real-time data.
- **Agent historical data:** Check to enable the flow of agent historical data from the peripheral to the Administration & Data Server. Uncheck to disable the flow of agent historical data.

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

a) **Name**—An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.
b) **Timeout threshold**—The maximum time, in milliseconds, the routing client can wait for a response to a routing request.
c) **Late threshold**—The threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the Timeout threshold.
d) **Timeout limit**—The maximum time, in seconds, for which the routing client waits for a response. If the routing client receives no responses from the Unified CCE system within this limit, it terminates routing operation.
e) **Default media routing domain**— Retain the default value, which is **None**.
f) **Default call type**—Use this call type for any route request that does not match a defined call type mapping.

The drop-down list contains all configured call types. The Unified CCE uses the default call type for any routing request from the routing client that does not otherwise map to a call type. If you do not define a default call type for the routing client, the Unified CCE uses a general default call type if you define one through the System Information command.

g) **Configuration parameters**—Leave blank.
h) **Dialed Number/Label map**—Indicates whether only specific labels are valid for each dialed number associated with this routing client (when selected) or whether all labels associated with the routing client are valid for any dialed number (when not selected). Leave unchecked.
i) **Client Type**—Select as follows from the drop-down list:

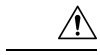
- For a CUCM PG: IPCC/Enterprise Agent
- For a VRU PG: VRU
- For an MR PG: MediaRouting
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

j) **Description**—More information about the routing client.
k) **Network routing client**—A name used to associate routing clients across instances.
l) **Network transfer preferred**—If this check box is checked, indicates that network transfer is preferred. When the target of a call is reachable by both a label defined for the requesting routing client and by another label defined for the network routing client that prerouted the call, this option indicates which choice is preferred.

Step 6 Click **Save**.

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

Configure Peripheral Gateway Setup



Caution To ensure that PGs work synchronously, configure the PGs that are collocated on the same physical server in the same order on both the sides. This must be based on the order in which they are installed and not on peripheral identifiers. For information on port utilization, refer to the *Port Utilization Guide for Cisco Unified Contact Center Solutions* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

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 Open the **Peripheral Gateway Setup** tool from Unified CCE Tools on the desktop.

Step 2 Click **Add** in the **Instance Components** section.

Step 3 Click **Peripheral Gateway**.

Step 4 Complete the following steps in the Peripheral Gateway Properties dialog box.

a) Choose **Production Mode**. Do not set the Auto Start feature until after the installation is complete.
b) Specify whether the PG is part of a duplexed pair.
c) In the ID field, select from the drop-down list the PG device number as enabled in the Router.
d) If the PG is duplexed, specify whether you are installing Side A or Side B. If the PG is simplex, select Side A.
e) In the **Client Type Selection** section of the window, select the client type:

- For a CUCM PG: CUCM
- For a MediaRouting PG: MediaRouting
- For a VRU PG: VRU
- For a UCC Enterprise Gateway PG: UCC Enterprise Gateway

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

Step 6 Enter the Logical Controller ID generated while configuring the PG in the **PG Explorer** tool. Click **Add** and select **PIM 1** from the list. Click **OK**.

Step 7 Configure the PG properties:

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

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

c) Enter the Peripheral ID in the **Peripheral ID** field. This is the ID that you created when you configured the PG in the PG Explorer tool.

d) For CUCM PG:

1. Enter the **Agent extension length**.
2. In the CUCM Parameters section, in the **Service** field, provide the IP address of the CUCM.
3. Enter the credentials of Application User that you created in CUCM.

   For more information about Application User, see Set Up Application User.
4. Select the appropriate **Mobile Agent Codec**, and click **OK**.

e) For MR PG:

- To add MR PG for ECE:

1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the ECE services server. If you have installed two services servers for high availability, provide the information for the primary service server on Side A.
2. In the **Application Connection Port (1)** field, enter the port number on the ECE services server that the PIM will use to communicate with the application. The default port is 38001.
3. In the **Application Hostname (2)** and **Application Connection Port (2)** fields, enter the hostname or the IP address of the secondary ECE services server VM and port number on Side B.

   Note Set these values only if you have installed two services servers for high availability.

- To add MR PG for Customer Collaboration Platform:

1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the Customer Collaboration Platform.
2. By default, Customer Collaboration Platform accepts the MR connection on Application Connection Port 38001. The Application Connection Port setting on Customer Collaboration Platform must match the setting on the MR PG as specified in the **Application Connection Port (1)** field.
3. Leave the **Application Hostname (2)** and **Application Connection Port (2)** fields blank.

- To add MR PG for Digital Routing service:

1. In the **Application Hostname (1)** and **Application Hostname (2)** fields, enter the hostname or the IP address of the Cloud Connect publisher and subscriber, respectively.

   Note Ensure to configure the **Application Hostname(1)** field to the network-nearest Cloud Connect. For example, if PIM-A is closer to the Cloud Connect publisher node, you must enter the IP address or hostname of the Cloud Connect publisher node in the **Application Hostname(1)** field and the IP address or hostname of the Cloud Connect subscriber node in the **Application Hostname (2)** field when configuring side "A".

2. In the **Application Connection Port (1)** and **Application Connection Port (2)** fields, retain the default port number, that is 38001, which is the fixed port for the Digital Routing service.

- To add MR PG for Outbound Option:

  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the BA_IP Dialer.
  2. In the **Application Connection Port (1)** field, enter the connection port for the BA_IP Dialer. Otherwise, accept the default port number (38001) on the application server machine that the PIM uses to communicate with the application.

- To add MR PG for any third-party application:

  1. In the **Application Hostname (1)** field, enter the hostname or the IP address of the multichannel application server machine.
  2. In the **Application Connection Port (1)** field, enter the port number on the application server that the PIM will use to communicate with the application. The default port is 38001.
  3. If two applications interact with the Unified CCE, in the **Application Hostname (2)** field, enter the hostname or the IP address of the second application server machine. If you are using the hostname, the name must be in the hosts file.
  4. For two applications that interact with the Unified CCE, in the **Application Connection Port (2)** field, enter the port number on the second application server machine that is used by the PIM.

The below steps are common for any application server:

1. For **Heartbeat Interval** (seconds), specify how often the PG checks its connection to the call server. Use the default value.
2. For **Reconnect Interval** (seconds), specify how often the PG should try to reestablish a lost connection to the call server. Use the default value.
3. Check the **Enable Secured Connection** checkbox to enable secured connection.

   Enable Secured Connection 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.

Note In case you are enabling ECDSA certificate, refer to the *How to enable ECDSA for Unified CCE core components* section in the Security Guide for Cisco Unified ICM/Contact Center Enterprise.

For more information, refer to the *Generate CVP ECDSA Certificate with OpenSSL* section in the Configuration Guide for Cisco Unified Customer Voice Portal.

f) For VRU PG:

1. In the **VRU host name** field, enter the name by which the VRU is known to the network.
2. In the **VRU connect port** field, enter the number of the VRU connection port that the PG connects to.

3. In the **Reconnect interval (sec)** field, specify how often, in seconds, the PG tries to re-establish a lost connection to the VRU. The default value is usually appropriate.
4. In the **Heartbeat interval (sec)** field, specify how often, in seconds, the PG checks its connection to the VRU. The default value is usually appropriate.
5. In the **DSCP** field, use the drop-down box to override the default value and set it to the desired DSCP value. The list of DSCP values in the drop-down box are the same as what are used during setup for connection between the Peripheral Gateway (PG) and the CallRouter. On an existing VRU PG system, this registry key does not exist. In that scenario, the PIM code uses CS3 as the default value when the VRU PIM process is activated.
6. Check the **Enable Secured Connection** checkbox to enable secured connection.

   This establishes a secured connection between VRU PIM and CVP.

Note In case you are enabling ECDSA certificate, refer to the topic *How to enable ECDSA for Unified CCE core components* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_12_6_1/configuration/guide/ucce_b_security-guide_12_6_1/ucce_b_security-guide_12_6_1_chapter_01000.html#Cisco_Task_in_List_GUI.dita_d28788be-b6ec-4017-922e-0eec9851df53

Step 8 Click **OK**.

Step 9 From the **Peripheral Gateway Component Properties** window, click **Next**. The **Device Management Protocol Properties** window appears.

a) Enter the appropriate settings and click **Next**. The **Peripheral Gateway Network Interfaces** window appears.
b) Configure the Private Interface and Public interfaces and click **Next**.

Note:

For the address input fields, use Fully Qualified Domain Names instead of IP addresses.

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

Step 10 In the **Check Setup Information window**, verify the setup information and click **Next**.

Step 11 When the **Setup Complete** window appears, click **Finish** .

Note When you add new PG, ensure that the PG ID is provided in the Router configuration. Provide the number that is assigned to the PG in the Enable Peripheral Gateway field in Web Setup

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 22.

Before you begin

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

Procedure

Step 1 Open a browser window on the PG machine.

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

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

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI for Windows**.We recommend you to download the 64 bit version. However, if you have already downloaded the 32 bit version, you can proceed to step 7.

Download the JTAPI plugin file.

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

Step 7 Open the installer.

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

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

Step 10 When prompted for the TFTP Server IP address, enter the CUCM IP address.

Step 11 Click **Finish**.

Step 12 Reboot the machine.

Install Cisco JTAPI Client on PG

Complete the following procedure only if you are installing JTAPI client to connect to Cisco Unified Communications Manager, Release 12.5 and above.

Before you begin

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

Procedure

Step 1 Open a browser window on the PG machine.

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

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

Step 4 Choose **Application** > **Plugins**. Click **Find**.

Step 5 Click the link next to **Download Cisco JTAPI Client for Windows** 64 bit or **Download Cisco JTAPI Client for Windows** 32 bit.

Download the JTAPI plugin file.

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

Step 7 Unzip the JTAPI plugin zip file to the default location or a location of your choice.

There are two folders in the unzipped folder `CiscoJTAPIx64` and `CiscoJTAPIx32`.

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

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

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

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

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

The JTAPI client installation completes at the default location. The following message is displayed:

```
Installation Complete.
```

Step 10 Reboot the machine.

What to do next

Note The default location, where the JTAPI client is installed, also contains the `uninstall64.bat` and `uninstall32.bat` file. Use this file to uninstall this version of the client, if necessary.

Set up CTI Server

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

Add CTI Server Component

Procedure

Step 1 Open Peripheral Gateway Setup tool from **Unified CCE Tools** on the desktop.

Step 2 Click **Add** in the Instance Components section.

The ICM Component Selection dialog box opens.

Step 3 Click **CTI Server**, and click **OK**.

The CTI Server Properties dialog box opens.

Set CTI Server Properties

Procedure

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

Note During Unified CCE installation on to Windows Server 2019, perform step 1 only after Unified CCE 12.6(2) for Windows Server 2019 and SQL Server 2019 support is installed.

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

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

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

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

Step 6 Click **Next**.

The CTI Server Component Properties dialog box opens.

Set CTI Server Component Properties

The CTI Server Component Properties dialog box supports the following modes of connections:

- **Secured and Non-Secured Connection (Mixed-mode)**: Allows secured and non-secured connection between the CTI Server and the CTI clients.
- **Secured-Only Connection**: Allows secured connection between the CTI Server and the CTI clients.

Important Non-Secured only mode is not supported.

Note To enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see the chapter *Certificate Management for Secured Connections* in *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.

In the CTI Server Component Properties dialog box, setup automatically displays the default **Secured Connection Port** and the **Non-Secured Connection Port** values. Use these values or change them to the required port numbers. CTI clients use these ports to connect to the CTI Server.

If you have multiple CTI servers running on a single machine, each CTI server must use a different port number set for *Secured connection* and *Mixed-mode connection*.

Procedure

Step 1 Select the appropriate connection type.

a) For *Secured Connection*, check the **Enable Secure-Only Mode** check box.

This option disables the **Non-Secured Connection Port** field.

b) For *Mixed-mode connection*, ensure that the **Enable Secure-Only Mode** check box is unchecked.

This is the default connection mode.

Step 2 To ensure that an agent is logged in to the client before the client receives events from the CTI Server, check the **Agent Login Required for Client Events** check box. This ensures that the clients are prevented from accessing data for other agents.

Step 3 Click **Next**.

The CTI Server Network Interface Properties dialog box opens.

Note In case your enabling ECDSA certificate, refer to the topic *How to enable ECDSA for Unified CCE core components* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

Set CTI Server Network Interface Properties

Procedure

Step 1 In the CTI Server Network Interface Properties dialog box, in the **PG public interfaces** section, enter the public network addresses for the PGs associated with the CTI Server.

Step 2 In the **CG private interfaces** section, enter the private network addresses of the CTI Server.

Step 3 In the **CG visible interfaces** section, enter the public network addresses of the CTI Server.

Step 4 Click **Next**.

The Check Setup Information window opens.

Complete CTI Server Setup

Procedure

Step 1 In the Check Setup Information window, ensure that the settings displayed are as you intended. If you want to modify any settings before proceeding, use the **Back** button.

Step 2 When the settings are correct, click **Next**.

Step 3 The final screen displays and asks whether you want to start the Node Manager now.

Step 4 Click **Finish** to exit setup (and optionally start the Node Manager).

If you choose to start it, the Node Manager automatically starts the other Unified CCE processes on the CTI Server.

Install Unified CCE Administration Client

Install Administration Client

Don't install the Administration Client on a system that already has other Unified CCE software installed; the Administration Client must reside on a standalone machine. **AdminClientInstaller** is available in the Unified CCE Installer ISO image and Minor Release installer.

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

Note

- Unified CCE 12.6(2) installs .Net Framework 4.8.

Procedure

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

Step 2 Launch 12.5 **AdminclientInstaller** from **AdminClientInstaller** folder.

The Administration Client Installer program proceeds through a series of screens on which you specify information.

Step 3 To apply the Unified ICM 12.6(2) Maintenance Release, click **Browse** and navigate to the Maintenance Release Software. Click **Next**.

Note You can also proceed with the installation of Administration Client 12.5(1) without selecting the Unified ICM 12.6(2) installer in this step. After installing Unified ICM 12.5(1), double-click the Unified ICM 12.6(2) installer, and proceed from step 5.

Step 4 When the installation is complete, reboot the server.

Step 5 Log in to your system using domain credentials with administrative privileges. The Unified CCE 12.6(2) installation wizard launches. Click **Next** to proceed.

Step 6 Select the radio button to accept the license agreement and click **Next**.

Step 7 Click **Install** to begin the installation.

Step 8 Select the radio button to restart the system and click **Finish**.

Set Up Administration Client

You can't run the Administration Client Setup tool remotely through a browser. Run the tool on the local machine. You must log in to the local machine with the system Administrator account. Configure Microsoft Chromium Edge as the default browser before launching Administration Client.

Before you begin

To view the lists and to perform tasks with the Administration Client Setup tool, you must have the following permissions:

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

Procedure

Step 1 Open the Administration Client Setup tool from Unified CCE Tools shortcut on the desktop.

Step 2 Sign in as a domain user with local Administrator rights.

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

Step 4 On the **Add Instance** page, from the drop-down list, choose the customer facility and instance.

Step 5 Enter an instance number.

The same instance name can occur more than once in a domain, so the instance number provides the uniqueness. The instance number must be 0–24. The instance number must match for the same instance across your entire deployment. For an Enterprise (single instance) deployment, select 0 unless there's a reason to choose another value.

Step 6 Click **Save**.

Step 7 Select **Component Management** > **Administration Clients**.

Step 8 Click **Add**.

Step 9 Select an instance for the Administration Client from the drop-down list.

Step 10 Click the radio button for your Administration Client type.

Step 11 Enter the hostname or IP address of the Primary and Secondary Administration & Data Servers. If you have only one Administration & Data Server, specify it for both Primary and and Secondary Administration & Data Servers; both fields are required.

Step 12 Click **Save**.

Install Unified CCE Language Pack

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

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

These tool sets include some of the following tools:

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

Note Unified CCE 12.6(2) has a separate language pack.

Java Upgrades

During installations and upgrades, Unified CCE installs the base required Java version.

You can apply Java updates to your contact center as follows:

- Apply Java updates for the latest 32-bit Java 8 minor version.

  For the most current Java support information, see the Contact Center Enterprise Compatibility Matrix at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html.

  You can download and install the OpenJDK Java updates from the OpenLogic website.

- Modify the Windows CCE_JAVA_HOME environment variable to point to the new OpenJDK Java Runtime Environment (JRE) location if it has changed.

Note AppDynamics machine agent that is packaged with Unified ICM and Unified CVP uses a separate copy of OpenJDK. Any vulnerability fix for OpenJDK requires an upgrade of the AppDynamics machine agent. This update is delivered through an engineering special (ES) for Unified ICM and Unified CVP.

Upgrade OpenJDKUtility

The Cisco Upgrade OpenJDKUtility:

- Upgrades OpenJDK JRE to latest release.
- Supports upgrade for both MSI and Zip file formats.
- Automatically sets the CCE_JAVA_HOME environment variable to updated version so that Unified CCE applications can employ the latest OpenJDK version as the Java runtime.

Before using the tool:

- Download the OpenJDK installer from the OpenLogic OpenJDK website: https://www.openlogic.com/openjdk. (Both msi and zip formats are supported).
- Copy the downloaded file into the Unified CCE component VMs. *For Example* **C:\UpgradeOpenJDKTool**.
- Download the utility from https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(2) and unzip **OpenJdkUpgradeTool.zip** to any local folder. For example: Download and Unzip under **C:\UpgradeOpenJDKTool**.
- Run **openJDKUtility.exe** from unziped folder For all the supported commands and for more details, refer to the *Readme.html* (which is available as part of the *OpenJdkUpgradeTool.zip*).

  Once the installation is successful, **CCE_JAVA_HOME** is updated and does not trigger the system reboot.

Upgrade Tomcat Utility

Use the optional Cisco Upgrade Tomcat Utility to:

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

  Tomcat uses the following release numbering scheme: Major.minor.build. For example, you can upgrade from 9.0.22 to 9.0.69. You cannot use this tool for major or minor version upgrades.

Before using the tool:

- Download the Tomcat installer (apache-tomcat-version.exe) from the Tomcat website: http://archive.apache.org/dist/tomcat/tomcat-9/. Copy the installer onto the Unified CCE component VMs. For Example C:\UpgradeTomcatTool.

- Download the utility zip file, extract it, and run the batch file to upgrade Tomcat.

  Download link: https://software.cisco.com/download/home/284360381/type/284416107/release/12.6(2)

- Delete or back up large log files in these directories to reduce upgrade time:

  <ICM install directory>:\icm\tomcat\logs
  <ICM install directory>:\icm\debug.txt

Install Tomcat

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

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

Procedure

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

Step 2 Enter this command to run the tool: **tomcatutility.bat**.

Step 3 When prompted, enter the full pathname of the Tomcat installer version you want to use.

For example:

```
c:\tomcatInstaller\apache-tomcat-9.0.69.exe
```

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

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

Note If the latest installed Tomcat does not work properly, install the previous working version using the Tomcat utility by following the above-mentioned steps.

Silent Installation

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

Silent Installation Prerequisites for Unified CCE Release 12.5(1)

Before running a silent installation, complete the following tasks:

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

  To override this default, edit the ICMCCSilentsetup.ini file in the ICM-CCE-Installer directory.
- Mount the ISO image to the target machine, and make the following edits on the target machine:

- If you are performing a Technology Refresh upgrade, change the **szInstallType** from **0** to **1**. The default value of **0** is for a Fresh Install.
- If you are performing a Technology Refresh upgrade, provide a path for the **szExportedRegistryPath** parameter where the exported registry from source machine is placed.
- To change the drive on which you are installing the application, change the **szDrive** parameter. Replace C with the drive where you want to install.
- If you do not want to apply SQL Security Hardening, change the line that reads **szSQLSecurity=1** to **szSQLSecurity=0**.

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

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

Procedure

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

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

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

Installation starts. Upon successful installation, the server reboots.

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

Silent Installation Prerequisites for Unified CCE Release 12.6(2)

Before running a silent installation, complete the following tasks:

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

  For example, if the response file is created on a machine with Unified CCE services set to Manual and then run on a machine with those services set to Automatic, an additional dialog will open during the install (alerting you that the services have been set from Automatic to Manual). This unexpected dialog

will cause the install to terminate, potentially leaving the system in an invalid state that requires manual recovery.

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

Procedure

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

Example:

```
"c:\ICM12.6(2).exe" -r -f1 c:\myanswerfilename.iss
```

The -r flag is for recording the response file.

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

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

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

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

Example:

```
"c:\ICM12.6(2).exe" -s -f1 c:\myanswerfilename.iss -f2 c:\silentinstall.log
```

The -f2 flag creates a log file.

What to do next

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

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

Set Deployment Type in Unified CCE Administration Configuration

Perform the following steps to set the deployment type.

For more information on deployment types, see the following document:

Solution Design Guide for Cisco Unified Contact Center Enterprise at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_list.html

Procedure

Step 1 On Administration & Data Server, from the desktop open the **Unified CCE Tools** folder and navigate to: **Administration Tools** > **CCE Web Administration** .

Step 2 Log in as a *Config* security group member in the format user@domain.

Step 3 Double-click **Unified CCE Administration**.

Step 4 Click **Infrastructure Settings** > **Deployment Settings**.

Step 5 On the **Deployment Type** page, select your deployment from the drop-down menu and click **Next**.

Step 6 Click **Done**.

What to do next

Set the principal AW and configure it with the Diagnostic Framework Service domain, username, and password if you have not already.

Cisco Finesse Server Installation

Cisco Finesse server is installed on a virtual machine (VM). The installation runs from an ISO image and uses an OVA template. For more information, see *Cisco Finesse Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-installation-guides-list.html.

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

The installation takes about an hour. For most of that time, it can run unattended. Much of the installation requires no action on the part of the person who runs it. When user input is required, use the following keyboard navigation and selection actions. The installation wizard screens do not recognize a mouse or a touchpad.

To do this	Press this key
Move to the next field.	Tab
Move to the previous field.	Alt-Tab
Select an option.	Spacebar
Scroll up or down a list.	Up or Down Arrow keys
Go to the previous screen.	Tab to Back and press the Spacebar
Get information about a screen.	Tab to Help and press the Spacebar

Installation Task Flow

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

1	Install Finesse on the primary node.	See Install Finesse on Primary Node, on page 34.
2	Configure the database settings.	See Configure Contact Center Enterprise Administration and Data Server Settings, on page 37.
3	Configure the CTI server settings.	See Configure Contact Center Enterprise CTI Server Settings
4	Restart Cisco Finesse Tomcat on the primary node.	See Restart Cisco Finesse Tomcat, on page 41.
5	Validate configuration	See Validate Configuration, on page 41
6	Configure the cluster settings for the secondary node.	See Configure Cluster Settings, on page 42.
7	Install Finesse on the secondary node.	See Install Finesse on Secondary Node, on page 42.
8	Ensure replication is functioning between the two nodes.	See Check Replication Status, on page 45.
8	Install language packs (optional).	See Install language pack.
9	Install VMware Tools	See Install VMware Tools for VOS, on page 63

Install Finesse on Primary Node

Procedure

Step 1 Follow the instructions in the OVA README.txt file to import and deploy the OVA, to edit VM settings, and to power on the VM and edit the BIOS settings in the console. For more information, see the section on *Installation Files*.

Note Do not use Thin Provisioning or a VM snapshot when creating a VM to host Cisco Finesse. The use of Thin Provisioning or snapshots can negatively impact the performance of Cisco Finesse operation.

Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

Step 2 Select **OK** on the Disk Found screen to begin the verification of the media integrity and a brief hardware check.

If the media check passes, select **OK** to open the Product Deployment Selection screen. Continue to Step 3.

If the media check fails, the installation terminates.

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

Select **OK** to open the Proceed with Install screen.

Step 4 The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE.

Select **Yes** on the Proceed with Install screen to open the Platform Installation Wizard screen.

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

Step 6 Select **Continue** on the Basic Install screen to open the Basic Install wizard.

The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.

The first Basic Install wizard screen is Timezone Configuration.

Step 7 On the Timezone Configuration screen:

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

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

The MTU Configuration screen appears.

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

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

Your selection of No opens the Static Network Configuration screen.

Step 10 On the Static Network Configuration screen, enter static network configuration values as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Host Name**.
b) Enter the **IP Address**.
c) Enter the **IP Mask**.
d) Enter the **GW Address**.
e) Select **OK** to open the Domain Name System (DNS) Client Configuration screen.

Step 11 On the DNS Client Configuration screen, select **Yes** to specify the DNS client information.

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

Step 12 Specify your DNS client information as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Primary DNS** (mandatory).
b) Enter the **Secondary DNS** (optional).
c) Enter the **Domain** (mandatory).
d) Select **OK** to open the Administrator Login Configuration screen.

Step 13 On the Administrator Login Configuration screen:

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

Step 14 On the Certificate Information screen:

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

Step 15 On the First Node Configuration screen, select **Yes** to indicate that you are configuring the first node.

Your selection of Yes opens the Network Time Protocol Client Configuration screen.

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

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

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

Step 19 On the Application User Configuration screen, enter the credentials for the application user.

Select **OK** to open the Platform Configuration Confirmation screen. This screen states that the platform configuration is complete.

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

The installation begins.

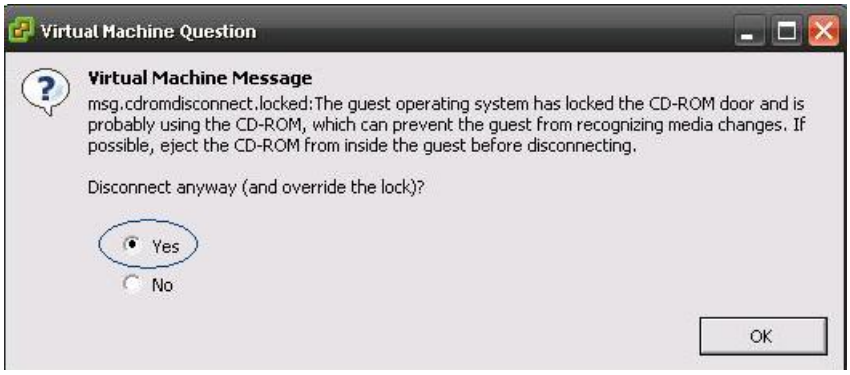
The installation can take up to an hour to complete and can run unattended for most of that time.

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

- Formatting progress bars
- Copying File progress bar
- Package Installation progress bars
- Post Install progress bar
- Populate RPM Archive progress bar
- Application Installation progress bars (multiple Component Install screens, security checks)
- An informational screen saying the system will reboot momentarily to continue the installation

  If you see the following virtual machine question, select **Yes**, and then click **OK**:

Figure 1: Virtual Machine Message



- A system reboot

Messages stream down your monitor during the reboot. Some of them prompt you to press a key. *Do not* respond to these prompts to press a key.

- Application Pre Install progress bars
- Configure and Setup Network progress bars

Note If a Network Connectivity Failure screen appears during the Configure and Setup Network process, click **Review**, and then click **OK** at the Errors screen. Follow the prompts to reenter the information that caused the failure. The installation continues when the connection information is complete.

- Security configuration

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

```
The installation of Cisco Finesse has completed successfully.

Cisco Finesse <version number>
<hostname> login: _
```

What to do next

Sign in to the Finesse administration console on the primary Finesse server (https://*FQDN of Finesse server:8445*/cfadmin) to configure CTI server, Administration & Database server, and cluster settings.

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

Configure Contact Center Enterprise Administration and Data Server Settings

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

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

Procedure

Step 1 Sign in to the administration console.

Step 2 In the Contact Center Enterprise Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the following table. Refer to your configuration worksheet if necessary.

Field	Description
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server. For example, **abcd12-5-aw-a**.

Field	Description
Backup Host/IP Address	The hostname or IP address of the backup Unified CCE Administration & Data Server. For example, **abcd12-5-aw-b**.
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	The domain name of the AWDB. For example, **cisco.com**.
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.

Step 3 Click **Save**.

Contact Center Enterprise CTI Server Settings

Use the Contact Center Enterprise CTI Server Settings gadget to configure the A and B Side CTI servers.

All fields on this tab are populated with default system values or with values an administrator has previously entered. Change values to reflect your environment and preferences.

For configuring secure connection select the Enable SSL encryption check box.

Test the CTI connection for given configuration using the **Test Connection** button.

Note After you make any changes to the values on the Contact Center Enterprise CTI Server Settings gadget, you must restart all the nodes of Cisco Finesse Tomcat. To make changes to other settings (such as Contact Center Enterprise Administration & Data Server settings), you can make those changes and then restart Cisco Finesse Tomcat.

If you restart Cisco Finesse Tomcat, agents must sign out and sign in again. As a best practice, make changes to CTI server settings and restart the Cisco Finesse Tomcat Service during hours when agents are not signed in to the Finesse desktop.

The secure encryption and Test Connection functionality is supported only from Unified CCE 12.5.

Note Although the B Side Host/IP Address and B Side Port fields are not shown as required, A and B Side CTI servers are mandatory for a production deployment of Unified CCE and Cisco Finesse.

The following table describes the fields on the Contact Center Enterprise CTI Server Settings gadget:

Field	Explanation
A Side Host/IP Address	The hostname or IP address of the A Side CTI server. This field is required. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.
A Side Port	The value of this field must match the port configured during the setup of the A Side CTI server. This field is required and accepts values between 1 and 65535. You can find this value using the Unified CCE Diagnostic Framework Portico tool on the PG box. For more information about Diagnostic Framework Portico, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise*. The default value is 42027.
Peripheral ID	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 server. This field is required and accepts values between 1 and 32767. The default value is 5000.
B Side Host/IP Address	The hostname or IP address of the B Side CTI server.

Field	Explanation
B Side Port	The value of this field must match the port configured during the setup of the B Side CTI server. This field accepts values between 1 and 65535.
Enable SSL encryption	Check this box to enable secure encryption.

Actions on the Contact Center Enterprise CTI Server Settings gadget:

- **Save:** Saves your configuration changes.
- **Revert:** Retrieves the most recently saved server settings.
- **Test Connection:** Tests the CTI connection.

CTI Test Connection

When you click **Test Connection**:

1. Input validation is done on the request attributes.

   Host/IP Address must not be empty. Port and Peripheral IDs must be within the valid range.

2. Validation is done to check if the provided Host/IP is resolved by Finesse box.
3. Validation is done to check if AW Database is reachable and if a valid path ID is configured for the provided Peripheral ID.
4. Socket connection is established to the provided Host/IP and port. The connection might fail if there is no route to the provided IP. If SSL encryption box is checked, this step also checks for successful TLS handshake. For TLS handshake to be successful, mutual trust has to be established between Finesse and CTI server.

   For information on how to establish trust between Finesse and CTI server, 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

5. After successful socket connection, a CTI initialization request is sent to check if the provided host is a CTI host.

   If the CTI response is a success for the CTI initialization request and peripheral provided is configured with Unified CCE, it is confirmed to be a CTI host.

6. CTI connection is closed by sending a CTI session close request.

Note If **Test Connection** is successful for Side A or B of the CTI cluster and the other side fails, it is a valid configuration as CTI server works in active-passive mode and connects to the active node. Inactive CTI node will refuse connection on the CTI port. However, Administrator has to ensure that the failed side also has a valid entry for CTI host and port field. System cannot verify this due to server restrictions.

If **Test Connection** is successful on Side A and B of the CTI cluster, then there is an error in the system configuration. Verify that the Side A and B of the CTI node have valid entries for port and host.

Test connection API success result does not guarantee peripheral to be online. It only validates if the peripheral provided is configured with Unified CCE.

Test connection API with insecure connection parameter will function as intended for earlier versions of Unified CCE deployments.

Restart Cisco Finesse Tomcat

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

Note After you restart Finesse, it can take approximately 6 minutes for all server-related services to restart. Therefore, you wait 6 minutes before you attempt to access the Finesse administration console.

Procedure

Step 1 Access the CLI and run the following command:

utils service restart Cisco Finesse Tomcat

Step 2 You can enter the command **utils service list** to monitor the Cisco Finesse Tomcat Service. After Cisco Finesse Tomcat changes to STARTED, the configured agents can sign in to the desktop.

Validate Configuration

After starting the Tomcat service, you must test the configuration for the changes you have made.

Procedure

Step 1 Log in to the GUI

Step 2 Click **Test** to test the configuration changes.

Validation errors, if any, in the configuration are displayed.

If there are any errors, you must restart the Tomcat service after you resolve the errors.

Configure Cluster Settings

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

Procedure

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

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

Step 3 Click **Save**.

Install Finesse on Secondary Node

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

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

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

Before you begin

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

Procedure

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

Messages appear while the preinstallation script runs. When the preinstallation script ends, the DVD Found screen opens.

Step 2 Select **Yes** on the DVD Found screen to begin the verification of the media integrity and a brief hardware check.

If the media check passes, select **OK** to open the Product Deployment Selection screen. Continue to Step 3.

If the media check fails, the installation terminates.

Step 3 The Product Deployment Selection screen states that the Cisco Finesse product suite will be installed. This screen has only one option: **OK**.

Select **OK** to open the Proceed with Install screen.

Step 4 The Proceed with Install screen shows the version of the product that is currently installed (if any) and the version of the product for this ISO. For the initial installation, the version currently installed shows NONE.

Select **Yes** on the Proceed with Install screen to open the Platform Installation Wizard screen.

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

Step 6 Select **Continue** on the Basic Install screen to open the Basic Install wizard.

The Basic Install wizard presents a series of screens that present questions and options pertinent to the platform and the setup configuration. Help is available for each wizard screen.

The first Basic Install wizard screen is Timezone Configuration.

Step 7 In the Timezone Configuration screen:

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

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

The MTU Configuration screen appears.

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

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

Your selection of No opens the Static Network Configuration screen.

Step 10 On the Static Network Configuration screen, enter the static network configuration values as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Host Name**.
b) Enter the **IP Address**.
c) Enter the **IP Mask**.
d) Enter the **GW Address**.
e) Select **OK** to open the Domain Name System (DNS) Client Configuration screen.

Step 11 On the **DNS Client Configuration** screen, select **Yes** to specify the DNS client information.

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

Step 12 Specify your DNS client information as follows, referring to the Configuration Worksheet if necessary:

a) Enter the **Primary DNS** (mandatory).
b) Enter the **Secondary DNS** (optional).
c) Enter the **Domain** (mandatory).

d) Select **OK** to open the Administrator Login Configuration screen.

Step 13 On the Administrator Login Configuration screen:

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

Step 14 On the Certificate Information screen:

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

Step 15 On the First Node Configuration screen, select **No** to indicate that you're configuring the second node.

A warning message appears that indicates you must first configure the server on the first node before you can proceed. If you already configured the first node, select **OK**.

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

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

a) Enter the **Host Name** of the primary Finesse server.
b) Enter the **IP Address** of the primary Finesse server.
c) Enter the **Security Password** of the primary Finesse server.
d) Confirm the **Security Password**.

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

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

The installation begins.

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

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

```
The installation of Cisco Finesse has completed successfully.

Cisco Finesse <version number>
<hostname> login: _
```

What to do next

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

After installation, by default the configuration that controls the reverse-proxy authentication is enabled. When the reverse-proxy authentication is enabled and multiple client-side certificates are configured on the system, it impacts the certificate acceptance pop-ups from clients that are connected directly to the Finesse server without using a reverse-proxy. To prevent these pop-ups from appearing, use the **utils systems reverse-proxy client-auth** command on both the Finesse nodes to disable the reverse-proxy authentication that don't need VPN-less access to Finesse.

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

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

Check Replication Status

Procedure

Step 1 Access the CLI on the primary Finesse server.

Step 2 Sign in with the Administrator User credentials that are defined during installation.

Step 3 Run the following command:

utils dbreplication runtimestate

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

Install Cisco Identity Service Standalone Deployment

Follow this sequence of tasks to install the Cisco Identity Service (Cisco IdS) standalone deployment.

Sequence	Task
1	Verify that you created a separate virtual machine for the IdS publisher node and the IdS subscriber node. See Set Up Virtual Machines.
2	Install IdS publisher node. See Install Publisher/Primary Node of Cisco Identity Service , on page 45
3	Set IdS subscriber node. See Set IdS Subscriber Node, on page 47
4	Install IdS subscriber node. See Install Subscriber/Secondary Node of Cisco Identity Service , on page 47
5	Upgrade VMware Tools. See Install VMware Tools for VOS, on page 63

Install Publisher/Primary Node of Cisco Identity Service

Before you begin

DNS Configuration is mandatory for installation of Cisco Identity Service. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Note If the deployment uses host files in addition to DNS, use FQDNs in the host file.

Procedure

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

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

Step 3 Select the virtual machine and power it on.

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

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Cisco Identity Service** and click **OK**.
d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

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

i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
n) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the **First Node Configuration** screen, select **Yes**.
q) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
r) In the **Security Configuration** screen, enter the security password and select **OK**.
s) In the **SMTP Host Configuration** screen, select **No**.
t) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
u) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

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

Step 5 Unmount the ISO image.

Set IdS Subscriber Node

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

Procedure

Step 1 Log in to your publisher IdS node.

Step 2 Run the following command to set the subscriber node:

set ids subscriber *name*
name
Specifies the hostname or ip address of the IdS subscriber node address.

What to do next

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

Required Minimum Privilege Level: Ordinary

Use this command to show IdS subscriber node information.

show ids subscriber

There are no required parameters.

Required Minimum Privilege Level: Advanced

Use this command to unset IdS subscriber node configuration.

unset ids subscriber

There are no required parameters.

Install Subscriber/Secondary Node of Cisco Identity Service

Before you begin

DNS Configuration is mandatory for installation of Cisco Identity Service. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Note If the deployment uses host files in addition to DNS, use FQDNs in the host file.

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

Procedure

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

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

Step 3 Select the virtual machine and power it on.

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

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Cisco Identity Service** and click **OK**.

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

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

Note For Live Data servers, use the same time zone for all the nodes.

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

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

Step 6 Unmount the ISO image.

Live Data Standalone Installation

Follow this sequence of tasks to install Live Data Standalone.

Sequence	Task
1	For all deployments except the 2000 agent reference design, verify that you created a separate virtual machine for the IdS publisher node and the IdS subscriber node. See Set Up Virtual Machines.
2	Install Live Data Primary Node. See Install Publisher/Primary Node of Live Data , on page 49
3	Set Live Data Secondary Node, on page 50
4	Install Live Data Secondary Node. See Install Subscriber/Secondary node of Live Data , on page 51
5	Upgrade VMware Tools. See Install Vmware Tools.
6	See *Configure Live Data with AW* section in the chapter "Upgrade from a Standalone Deployment to a Coresident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)."
7	Configure Live Data Machine Services, on page 52
8	Configure Live Data for Unified Intelligence Center Data Sources, on page 53
9	Restart Live Data, on page 54
10	Set Up Certificates for Live Data, on page 54

Install Publisher/Primary Node of Live Data

Before you begin

DNS Configuration is mandatory for installation of Live Data. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

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

Procedure

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

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

Step 3 Select the virtual machine and power it on.

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

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Live Data** and click **OK**.
d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

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

i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
n) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the **First Node Configuration** screen, select **Yes**.
q) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
r) In the **Security Configuration** screen, enter the security password and select **OK**.
s) In the **SMTP Host Configuration** screen, select **No**.
t) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
u) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

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

Step 5 Unmount the ISO image.

Set Live Data Secondary Node

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

Procedure

Step 1 Log in to your primary Live Data node.

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

set live-data secondary *name*
name

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

Install Subscriber/Secondary node of Live Data

This task is required for installation of the DNS Configuration is mandatory for installation of Live Data. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Before you begin

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

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

Procedure

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

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

Step 3 Select the virtual machine and power it on.

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

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, select **Live Data** and click **OK**.

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

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

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

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.

k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

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

Step 6 Unmount the ISO image.

Configure Live Data Machine Services

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

Note

- Whenever you run set live-data machine-services, be sure to also run set live-data cuic-datasource to reconfigure the Live Data data sources for the Unified Intelligence Center. See Configure Live Data for Unified Intelligence Center Data Sources, on page 53.
- If you are using any certificates that are unapproved by Cisco or self-signed certificate, ensure to import the AWDB certificate into the Live Data server before you run set live-data machine-services.

Procedure

Step 1 Log in to your Live Data server.

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

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

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

Note

- The Router and Peripheral Gateway (PG) TIP and TOS connection information is automatically populated for Unified CCE deployments that support Live Data. To set the deployment type, see Set Deployment Type in Unified CCE Administration Configuration, on page 32. The Live Data server uses this information to establish a connection, and receive reporting data as well as agent and call events as they occur.
- Cisco Unified Communications Manager (CUCM) PG, generic PGs with CUCM peripherals, and Unified CCE Gateway PGs are supported for Live Data.

Note Once you have updated the host name of Live Data Server, you need to re-run the below set of commands, otherwise new host name will not be accepted.

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

set live-data cuic-datasource *cuic-addr cuic-port cuic-user*

Verify that the show machine-services display changed hostname.

It is necessary for you to re-run the set of commands, otherwise Live data machine services will not be updated with the new host name.

Configure Live Data for Unified Intelligence Center Data Sources

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

Note If you are using any certificates that are unapproved by Cisco, ensure to import the CUIC certificate into the Live Data server before you run set live-data machine-services.

Procedure

Step 1 Log in to your Live Data server.

Step 2 Run the following command to configure your Live Data Unified Intelligence Center data sources:

set live-data cuic-datasource *cuic-addr cuic-port cuic-user*

Configure Cross Origin Resource Sharing (CORS) for Live Data

Live Data CORS commands allow you to configure CORS and hence allow web applications running on different origins to communicate with Live Data and CUIC.

For Unified Intelligence Centre gadgets (Live Data) to load in Cisco Finesse, ensure to:

- Enable CORS using `utils cuic cors enable` and `utils live-data cors enable` commands.
- Set the Finesse host URL in `utils cuic cors allowed_origin add URLs` and `utils live-data cors allowed_origin add URLs` commands.

Examples:

- https://<finesse-FQDN>
- https://<finesse-FQDN>:port

For more information on CUIC CORS CLIs, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html

Restart Live Data

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

Procedure

Access the Live Data CLI and run the following command:

utils system restart

Note Whenever a new peripheral gateway that supports Live Data gets deployed and started, its feed will not be available to Live Data server automatically. Restart the Live Data server to start the feed from the newly deployed Peripheral Gateway.

Set Up Certificates for Live Data

For secure Cisco Finesse, Cisco Unified Intelligence Center, AWDB, and Live Data server-to-server communication, perform any of the following:

- Use the self-signed certificates provided with Live Data.

Note When using self-signed certificates, agents must accept the Live Data certificates in the Finesse desktop when they sign in before they can use the Live Data gadget.

- Produce a Certification Authority (CA) certificate internally.
- Obtain and install a Certification Authority (CA) certificate from a third-party vendor.

For complete information

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

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

Sequence	Task
1	Set Deployment Type in Unified CCE Administration Configuration: Set Deployment Type in Unified CCE Administration Configuration, on page 32
2	Install Coresident Deployment Primary Node. See Install Publisher/Primary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 55
3	Install Coresident Deployment Secondary Node. See Install Subscriber/Secondary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS), on page 57
4	Add Coresident (Cisco Unified Intelligence Center with Live Data and IdS) Machine Type to the System Inventory, on page 58
5	Upgrade VMware Tools. See Install Vmware Tools.
6	
7	Configure Live Data Unified Intelligence Center Data Sources, on page 59
8	Restart Live Data, on page 59
9	Set up certificates for Live Data. See

Note From Cisco Finesse Release 12.5(1) or later, Cisco Unified Intelligence Center supports XML gadgets. Switching to XML based gadgets reduces latency and improves performance.

After Cisco Unified Intelligence Center or Coresident deployment installation, run **utils finesse layout updateCuicGadgetUrl** command to optimize the loading of Cisco Unified Intelligence Center gadgets. This command allows you to change the .jsp references of Cisco Unified Intelligence Center gadgets to .xml with no functional changes.

Install Publisher/Primary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

Before you begin

DNS Configuration is mandatory for installation of Coresident deployment (Cisco Unified Intelligence Center with Live Data and IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

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

Procedure

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

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

Step 3 Select the virtual machine and power it on.

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

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, for the Progger (Lab only) or 2000 agent reference design, choose **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.
d) In the **Proceed with Install** screen, select **Yes**.
e) In the **Platform Installation Wizard** screen, select **Proceed**.
f) In the **Apply Patch** screen, select **No**.
g) In the **Basic Install** screen, select **Continue**.
h) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

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

i) In the **Auto Negotiation Configuration** screen, select **Continue**.
j) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the **DHCP Configuration** screen, select **No**.
l) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
m) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
n) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the **First Node Configuration** screen, select **Yes**.
q) In the **Network Time Protocol Client Configuration** screen, enter a valid NTP server IP address and select **OK**.
r) In the **Security Configuration** screen, enter the security password and select **OK**.
s) In the **SMTP Host Configuration** screen, select **No**.
t) In the **Application User Configuration** screen, enter the application username. Enter, and confirm the application user password. Select **OK**.
u) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

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

Step 5 Unmount the ISO image.

Install Subscriber/Secondary Node of Co-resident Deployment (Cisco Unified Intelligence Center with Live Data and IdS)

Before you begin

DNS Configuration is mandatory for installation of Coresident deployment (Cisco Unified Intelligence Center with Live Data and IdS). To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

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

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

Procedure

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

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

Step 3 Select the virtual machine and power it on.

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

a) In the **Disk Found** screen, click **OK** to begin the verification of the media integrity.
b) In the **Success** screen, select **OK**.
c) In the **Product Deployment Selection** screen, for the Progger (Lab only) or 2000 agent reference design, choose **Cisco Unified Intelligence Center with Live Data and IdS**, and then select **OK**. The **Cisco Unified Intelligence Center with Live Data and IdS** option installs Cisco Unified Intelligence Center with Live Data and Cisco Identity Service (IdS) on the same server.

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

a) In the **Proceed with Install** screen, select **Yes**.
b) In the **Platform Installation Wizard** screen, select **Proceed**.
c) In the **Apply Patch** screen, select **No**.
d) In the **Basic Install** screen, select **Continue**.
e) In the **Timezone Configuration** screen, use the down arrow to choose the local time zone that most closely matches where your server is located. Select **OK**.

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

f) In the **Auto Negotiation Configuration** screen, select **Continue**.
g) In the **MTU Configuration** screen, select **No** to keep the default setting for Maximum Transmission Units.
h) In the **DHCP Configuration** screen, select **No**.
i) In the **Static Network Configuration** screen, enter static configuration values. Select **OK**.
j) In the **DNS Client Configuration** screen, enter your DNS client configuration. Select **OK**.
k) In the **Administrator Login Configuration** screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.

l) In the **Certificate Information** screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
m) In the **First Node Configuration** screen, select **No**.
n) In the warning screen, select **OK**.
o) In the **Network Connectivity Test Configuration** screen, select **No**.
p) In the **First Node Access Configuration** screen, enter the host name and IP address of the first node. Enter and confirm the security password. Select **OK**.
q) In the **SMTP Host Configuration** screen, select **No**.
r) In the **Platform Configuration Confirmation** screen, select **OK**. The installation begins and runs unattended.

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

Step 6 Unmount the ISO image.

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

Procedure

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

Step 2 Add the new machine to the System Inventory:

a) Click **Add**.

The **Add Machine** popup window opens.

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

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

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

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

d) Enter the machine's Administration credentials.
e) Click **Save**.

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

What to do next

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

Configure Live Data Unified Intelligence Center Data Sources

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

Before you begin

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

Procedure

Step 1 Log in to your Live Data server.

Step 2 Run the following command to configure your Live Data Unified Intelligence Center data sources:

set live-data cuic-datasource *cuic-addr cuic-port cuic-user*

Restart Live Data

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

Procedure

Access the Live Data CLI and run the following command:

utils system restart

Install Cloud Connect

Follow this sequence of tasks to install the Cloud Connect cluster.

Sequence	Task
1	Install Publisher or Primary Node of Cloud Connect. See, Install Publisher or Primary Node of Cloud Connect, on page 60
2	Set Cloud Connect Secondary Node. See, Set Subscriber or Secondary Node of Cloud Connect, on page 61
3	Install Subscriber or Secondary Node of Cloud Connect. See, Install Subscriber or Secondary Node of Cloud Connect, on page 61

Sequence	Task
4	Initial Configuration for Cloud Connect

Install Publisher or Primary Node of Cloud Connect

Before you begin

DNS Configuration is mandatory for installation of Cloud Connect deployment. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Note If the deployment uses host files in addition to DNS, use FQDNs in the host file.

Procedure

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

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

Step 3 Select the virtual machine and turn on the power.

Step 4 Follow the Install wizard and select appropriate values:

a) In the Disk Found screen, click **OK** to begin the verification of the media integrity.
b) In the Success screen, select **OK**.
c) In the Product Deployment Selection screen, choose **Cisco Contact Center Cloud Connect**, and then select **OK**.
d) In the Proceed with Install screen, select **Yes**.
e) In the Platform Installation Wizard screen, select **Proceed**.
f) In the Apply Patch screen, select **No**.
g) In the Basic Install screen, select **Continue**.
h) In the Timezone Configuration screen, use the down arrow to set the zone to Central Controller time. Select **OK**.
i) In the Auto Negotiation Configuration screen, select **Continue**.
j) In the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the DHCP Configuration screen, select **No**.
l) In the Static Network Configuration screen, enter static configuration values. Select **OK**.
m) In the DNS Client Configuration screen, enter your DNS client configuration. Select **OK**.
n) In the Administrator Login Configuration screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the Certificate Information screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the First Node Configuration screen, select **Yes**.
q) In the Network Time Protocol Client Configuration screen, enter a valid NTP server IP address and select **OK**.
r) In the Security Configuration screen, enter the security password and select **OK**.
s) In the SMTP Host Configuration screen, select **No**.

t) In the Application User Configuration screen, enter the application username. Enter and confirm the application user password. Select **OK**.
u) In the Platform Configuration Confirmation screen, select **OK**. The installation begins and runs unattended.

Note During installation, the system is rebooted automatically. On completing installation, a sign-in prompt is displayed.

Step 5 Unmount the ISO image.

Set Subscriber or Secondary Node of Cloud Connect

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

Procedure

Step 1 Sign in to your primary Cloud Connect node.

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

set cloudconnect subscriber [name]

name – Specifies the FQDN or IP address of the Cloud Connect subscriber node (maximum 255 characters).

Install Subscriber or Secondary Node of Cloud Connect

Before you install the subscriber or secondary node, you must install the publisher or primary node and configure the cluster.

Before you begin

DNS Configuration is mandatory for installation of Cloud Connect deployment. To configure DNS, add the VMs to the forward and reverse lookups of the DNS.

Note If the deployment uses host files in addition to DNS, use FQDNs in the host file.

Procedure

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

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

Step 3 Select the virtual machine and turn on the power.

Step 4 Follow the Install wizard and select appropriate values:

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

c) In the Product Deployment Selection screen, choose **Cisco Contact Center Cloud Connect**, and then select **OK**.
d) In the Proceed with Install screen, select **Yes**.
e) In the Platform Installation Wizard screen, select **Proceed**.
f) In the Apply Patch screen, select **No**.
g) In the Basic Install screen, select **Continue**.
h) In the Timezone Configuration screen, use the down arrow to set the zone to Central Controller time. Select **OK**.
i) In the Auto Negotiation Configuration screen, select **Continue**.
j) In the MTU Configuration screen, select **No** to keep the default setting for Maximum Transmission Units.
k) In the DHCP Configuration screen, select **No**.
l) In the Static Network Configuration screen, enter static configuration values. Select **OK**.
m) In the DNS Client Configuration screen, enter your DNS client configuration. Select **OK**.
n) In the Administrator Login Configuration screen, enter the Platform administration username. Enter and confirm the password for the administrator. Select **OK**.
o) In the Certificate Information screen, enter data to create your Certificate Signing Request: Organization, Unit, Location, State, and Country. Select **OK**.
p) In the First Node Configuration screen, select **No**.
q) In the warning screen, select **OK**.
r) In the Network Connectivity Test Configuration screen, select **No**.
s) In the First Node Access Configuration screen, enter the FQDN of the first node. Enter and confirm the security password. Select **OK**.
t) In the SMTP Host Configuration screen, select **No**.
u) In the Platform Configuration Confirmation screen, select **OK**. The installation begins and runs unattended.

Note During installation, the system is rebooted automatically. On completing installation, a sign-in prompt is displayed.

Step 5 Unmount the ISO image.

Note
- In case one needs to add a subscriber back to the cluster, you must run the **set command** and re-install the subscriber.
- If a new subscriber needs to be added, we have to remove the existing subscriber node using the **unset command** and then add the new subscriber node using the **set command**. After that we need to install the new subscriber node to form the cluster.

Initial Configuration for Cloud Connect

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

For more information, see the section *Certificates for CCE Web Administration* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

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

Step 2 In the Inventory page, click **New** to add the new machine to the System Inventory.

Step 3 In the Add Machine dialog box:

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

Note For more information on Cloud Connect installation and onboarding process, see CCE Orchestration section.

Note When you configure Cloud Connect Publisher, its Cloud Connect Subscriber is added to the Inventory automatically.

Install VMware Tools for VOS

To install or upgrade VMware Tools using VOS, perform the following steps:

Procedure

Step 1 Ensure that your virtual machine is powered on.

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

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

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

Step 5 Enter the command **utils vmtools refresh** and confirm.
The server automatically reboots twice.

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

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