Post Installation Configuration

Packaged CCE 2000 Agents Deployment

Follow this sequence to configure components for Packaged CCE 2000 Agents deployment.

Sequence	Task
1	Configure CCE Component, on page 2
2	Configure Cisco Unified Customer Voice Portal, on page 24
3	If Media Server is external, Configure Media Server
4	Configure Cisco Unified Communications Manager, on page 24
5	Configure Cisco Unified Intelligence Center, on page 31
6	Configure Cisco Finesse, on page 36
7	Configure Cisco Identity Service, on page 101
8	Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39 (optional)
9	Configure VVB, on page 43 (optional)
10	Configure Cisco IOS Enterprise Voice Gateway, on page 43
11	Configure IPv6, on page 50
12	Configure Enterprise Chat and Email (ECE) (optional) Email and Chat

Configure CCE Component

Follow this sequence to configure the core CCE components.

Sequence	Task
1	Configure SQL Server for CCE Components, on page 2
2	Set up Organizational Units, on page 2
3	Initialize the Packaged CCE 2000 Agents Deployment Type, on page 5
4	Add PIMs to the Media Routing Peripheral Gateway (optional)
5	Cisco SNMP Setup, on page 21 (optional)
6	For details on CA certificate, see Generate and Import CA Signed Certificate in AW Machine
7	For details on self-signed certificate, see Generate and Import Self-signed Certificate in AW Machine

Configure SQL Server for CCE Components

The following procedure must be done in Logger, Rogger, and AW Machines.

Procedure

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

Step 2 Log in.

Step 3 Expand **Security** and then **Logins**.

Step 4 If the BUILTIN\Administrators group is not listed:

a) Right-click **Logins** and select **New Login**.
b) Click **Search** and then **Locations** to locate BUILTIN in the domain tree.
c) Type **Administrators** and click **Check Name** and then **OK**.
d) Double-click **BUILTIN\Administrators**.
e) Choose **Server Roles**.
f) Ensure that **public** and **sysadmin** are both checked.

Set up Organizational Units

Add a Domain

Use the Domain Manager tool to add a domain. Perform the following steps only once on the AW server.

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 Users to Local Administrators Group

Repeat the following steps for all the Unified CCE servers, to add the domain user or domain group to the local Administrators group.

Note You can add a domain group to local Administrators group of the server to provide users in domain group administrative permission on the server, provided the users are immediate members of the domain group.

Procedure

Step 1 Click **Server Manager** > **Tools** > **Computer Management**.

Step 2 Select **Local Users and Groups**.

Step 3 Double-click **Groups**.

Step 4 Right-click **Administrators**. Select **Properties**.

Step 5 Click **Add** and enter the user name or domain group name in the **Edit the Object names to select** check box.

Step 6 Select **Check Names** to validate the names.

Step 7 After the name is successfully validated, click **OK**.

Step 8 Click **Apply** and **OK** in the **Properties** dialog box.

Step 9 Close the **Computer Management** and **Server Manager** windows.

Initialize the Packaged CCE 2000 Agents Deployment Type

Initialize the Packaged CCE deployment using Unified CCE Administration.

When you sign into Unified CCE Administration for the first time, you are prompted to enter information and credentials for the components in your deployment. Packaged CCE uses this information to configure the components and build the System Inventory.

If you are in the process of upgrading from an earlier release, Packaged CCE prompts you only for missing information and credentials; you may not need to perform each step.

Note After a Packaged CCE deployment is initialized, you cannot switch to another deployment type.

Note The system does not support IP address change. This is applicable for all the **Hostname/ IP Address** fields.

Procedure

Step 1 Sign into **Unified CCE Administration** using the Active Directory username (*user@domain*) and password (`https://<IP Address>/cceadmin`, where <IP Address> is the address of the Side A Unified CCE AW-HDS-DDS).
The **Configure your deployment** popup window opens automatically.

Step 2 On the **Deployment Type** page, select a **Deployment Type** and an **Instance** from the respective drop-down lists. You must be a member of the Setup security group for the instance you select. Click **Next**.

Step 3 On the **VM Host** page, enter the IP address, Username, and Password for the VMware hosts for Side A and Side B.

The VMware hosts are the two servers on which ESXi is installed. The username and password fields are the host login names and passwords configured in ESXi.

- If you do not want to use the "root" user credentials. You can create user with the following permissions:

Users must have *Read* and *Reboot* permissions on the hosts. To enable these permissions in the VMware Host Client, set the following in **Manage Permissions**:

- *Anonymous*, *View*, and *Read* in **Root** > **System** (enabled by default).
- *Reset* in **Root** > **VirtualMachine** > **Interact**.

Note If you update the ESXi root password in Packaged CCE 2000 agent deployment, be sure to reinitialize the deployment in the Inventory page.

Step 4 Select the hardware layout type as **M3/M4 Tested Reference Configuration** or **M5 Tested Reference Configuration / Specification Based Configuration** and click **Next**.

Packaged CCE validates the hosts in your deployment.

- If you select **M3/M4 Tested Reference Configuration**, the system checks if the hardware is supported UCS hardware and verifies if the VMs are configured as per the reference design. If the validation is successful, the **Credentials** page opens.
- If you select **M5 Tested Reference Configuration / Specification Based Configuration**, the system validates the hardware specifications of the VMware host and verifies if the VMs are configured as per the reference design. If the validation is successful, click **Next** to open the **Credentials** page. See the *Virtualization for Cisco Packaged CCE* at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/virtualization/pcce_virt_index.html for hardware specifications.

  Note

  - Datastores used by Cisco VMs should not be shared or used by other third-party VMs.
  - Packaged CCE core components include:
    - Unified CCE Rogger
    - Unified CCE AW/HDS/DDS
    - Unified CCE PG
    - Unified CVP Server
    - Unified Intelligence Center Publisher (with coresident Live Data and IdS)
    - Finesse

    VM annotations are used to identify Packaged CCE core component VMs. Do not change the default annotations of any of the core component VMs. The following terms are reserved for core component annotations: Cisco, Finesse, CUIC, and CVP. Do not use these reserved terms in the annotations of any of the non-core component VMs.
  - Core components must be on-box, all other components have to be added as external machines. For more information, see the *Add External Machines* topic in the *Cisco Packaged Contact Center Enterprise Administration and Configuration Guide, Release 11.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html
  - All other non-core components are required to be added as an external machine in the Packaged CCE Inventory.

- If the validation fails, click **Update Hosts** to go back to the **VM Hosts** page and edit the values. Click **Retry** to run the validation with existing values.

Step 5 On the **Credentials** page, enter the specified information for each component in your deployment. After entering information for a component, click **Next**.

The system validates the credentials you entered before prompting you for the next component's information.

Component	Information Required
Unified CM	Either: • The Unified CM Publisher for an on-box Unified Communications Manager deployment. • The Unified CM Publisher Name and IP address for an external Unified Communications Manager deployment. **Note** • Only a single Unified CM cluster can be integrated to a single site of Packaged CCE deployment. • For **M3/M4 Tested Reference Configuration**, Unified CM 12.5 installation must be off-box. AXL username and password.
Unified CVP	Unified CVP Server (Side A) Windows Administration Username and Password. Unified CVP Server (Side B) Windows Administration Username and Password.
Unified CCE AW-HDS-DDS	Unified CCE Diagnostic Framework Portico domain, username, and password. These credentials must be of a domain user who is a local administrator on all the CCE servers and valid on all Unified CCE components in your deployment (the Side A and Side B Unified CCE Roggers, PGs, and AW-HDS-DDSs). **Note** Every time the Active Directory credentials are updated, the credentials configured here must be updated as well.
Unified Intelligence Center	Unified Intelligence Center Administration application username and password. Identity Service Administration username and password.
Finesse	Finesse Administration username and password.
CVP Reporting	**Note** This tab is available only if Unified CVP Reporting server is on-box for **M3/M4 Tested Reference Configuration**. Unified CVP Reporting Server Windows Administration Username and Password used during server installation.

Step 6 On the **Settings** page, select the following:

- Select the codec used for Mobile Agent calls from the **Mobile Agent Codec** drop-down menu. The codec you select must match the codec specified on the voice gateways.
- If you have an external Unified Communications Manager, select the Unified CM Subscribers to which the Side A and Side B Unified CCE PGs connect from the **Side A Connection** and **Side B Connection** drop-down menus.
- Enter the username and password for an existing Active Directory user in the same domain as the Packaged CCE servers. This account will be added to the Service group.

Click **Next**.

The deployment is initialized. The **Details** dialog box displays the status of the automated initialization tasks.

See Automated Initialization Tasks for Components, on page 8 for more information.

Step 7 After the automated initialization tasks complete, click **Done**.

If one of the automated initialization tasks fails, correct the errors and then click **Retry**.

If the retry is successful, the automated initialization continues.

For some task failures, all completed tasks must be reverted before the task can be retried. You see a message informing you that the system needs to be reverted to a clean state.

Click **OK**, and then after the system is in a clean state, click **Start Over**.

Note The System Inventory displays alerts for some machines when it opens after initialization completes and you click **Done**. These alerts will be cleared after you configure Unified Communications Manager.

What to do next

After you have configured the deployment, you can specify system-level settings. For example, you can enter labels for Unified Communications Manager, Unified CVP, and outbound calls. See Miscellaneous.

Automated Initialization Tasks for Components

Packaged CCE performs the following tasks during initialization.

Component	Automated Initialization Tasks
Unified CCE Rogger	• Creates the Logger. • Creates the Router.
Unified CCE PG	• Downloads JTAPI from the Unified Communications Manager, and installs it on the Unified CCE PG. • Creates the CUCM Peripheral Gateway (PG) with the CUCM PIM. • Creates the Media Routing PG (MR PG). • Creates the VRU PG with two VRU PIMs. • Creates the CTI Server.
Unified CCE AW-HDS-DDS	• Creates the AW-HDS-DDS. • Creates the Cisco Unified Intelligence Center SQL user account that is used for Unified Intelligence Center data sources. • Creates the Cisco Finesse SQL user account that is used for Cisco Finesse data sources.

Component	Automated Initialization Tasks
Unified Communications Manager	• Creates the Application User that is used to configure the Unified CCE PG.
Unified Customer Voice Portal	• Configures the Unified CVP Call Server. • Configures the Unified CVP VXML Server. • Configures the Unified CVP Media Server.
Unified CVP Reporting Server	• Initializes the Unified CVP Reporting Server.
Unified Intelligence Center	• Updates the historical and real-time data sources. • Disables the AW database synchronization
Cisco Finesse	• Configures the CTI Server settings. • Configures the connection to the AW database. • Disables the **Reasons** gadget in Finesse Administration.

System Inventory for Packaged CCE 2000 Agents Deployment

Note The System Inventory shows IPv4 addresses only.

The System Inventory is a visual display of the machines in your deployment, including: Virtual Machine Hosts (ESXi servers), Virtual Machines (VMs) on Side A, VMs on Side B, External Machines, Gateways, and Cisco Virtualized Voice Browsers (VVB). You can access the System Inventory after you have completed the change to a Packaged CCE deployment.

Access the System Inventory by navigating to **Unified CCE Administration** > **Infrastructure** > **Inventory**.

System Inventory contents are updated when you select or change the deployment type and after regular system scans. If a system scan detects VMs that do not conform to Packaged CCE requirements, the **Configure your deployment** pop-up window opens automatically, detailing the errors. You can access the System Inventory again after you have corrected the errors and completed the **Configure your deployment** pop-up window.

For more details about the Packaged CCE requirements, see **Server Status** pop-up window, see Monitor Server Status Rules for Packaged CCE 2000 Agents Deployment, on page 19.

Table 1: System Inventory Layout and Actions

Item	Notes	Actions
Validate	If a system scan detects an error or warning for validation rules, correct the error, and then click **Validate** to run an immediate scan and verify that you corrected the problem.	Click **Validate**.

Item	Notes	Actions
Side A	This panel shows all VMs on Side A.	

Item	Notes	Actions
		The System Inventory displays read-only information for the following VMs: • **Unified CCE Rogger** • **Unified CCE PG** • **Unified CM Subscriber 1**(if on-box) The following VMs are editable. Click the VM **pencil** icon to edit the following fields: **Note** If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory. • **Unified CCE AW-HDS-DDS**—Diagnostic Framework Service Domain, Username, and Password. • **Unified CM Publisher**(if on-box)—AXL Username and Password. These are the credentials for connecting to the Unified CM Publisher. • **CUIC-LD-IdS Publisher**—Username and Password for Unified Intelligence Center Administration. Username and Password for Identity Service Administration. • **Unified CVP Server**— Unified CVP Server Windows credentials. Configure FTP. For more information on the FTP attributes, see FTP Section in the Add Media Server as External Machine. • **Finesse Primary**—Username and Password for Cisco Finesse Administration. You can launch the administration tool for these VMs by clicking the VM **arrow** icon: • **CUIC-LD-IdS Publisher** • **Unified CM Publisher** You can perform the full synchronization or differential synchronization of the configurations of various components. For more information on the machines that support data synchronization, see Device Out of Sync Alerts. **Note** To enable CVP Statistics feature in Packaged CCE 12.0(1), install the ICM12.0(1) ES patch. For more information, see *Release*

Item	Notes	Actions
		Notes for Packaged Contact Center Enterprise at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html. You can launch statistics for the following VMs by clicking the **Statistics** icon: • **Unified CVP** • **Unified CVP Reporting** For more information, see Unified CVP Statistics and Unified CVP Reporting Statistics.

Item	Notes	Actions
Side B	This panel shows all VMs on Side B.	

Item	Notes	Actions
		The System Inventory displays read-only information for the following VMs: • **Unified CCE Rogger** • **Unified CCE PG** • **Unified CCE AW-HDS-DDS** • **Unified CM Subscriber 2**(if on-box) • **CUIC-LD-IdS Subscriber** • **Finesse Secondary** • ECE Data Server The following VMs are editable. Click the VM **pencil** icon to edit the following fields: **Note** If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory. • **Unified CVP** - Unified CVP Server Windows credentials. Configure FTP. For more information on the FTP attributes, see FTP Section in the Add Media Server as External Machine. • **Unified CVP Reporting** - Cisco Unified CVP Reporting Server Windows credentials. If the CVP Reporting server VM is re-imaged or re-installed, you need to initialize the CVP Reporting server. To initialize the CVP Reporting Server , click the Initialize icon and then click **Yes** to confirm. **Note** Initialization removes existing call server association and Courtesy Callback configuration. To re-associate call servers with CVP Reporting server, navigate to **Overview** > **Infrastructure Settings** > **Device Configuration** > **Device Configuration**. To reconfigure Courtesy Callback, navigate to **Overview** > **Features** > **Courtesy Callback**. You can perform the full synchronization or differential synchronization of the configurations of various

Item	Notes	Actions
		components. For more information on the machines that support data synchronization, see Device Out of Sync Alerts. You can launch statistics for the following VMs by clicking the **Statistics** icon: • **Unified CVP** • **Unified CVP Reporting** For more information, see Unified CVP Statistics and Unified CVP Reporting Statistics.

Item	Notes	Actions
External Machines		To add or update the external machines, see Add External Machines. You can perform the full synchronization or differential synchronization of the configurations of various components. For more information on the machines that support data synchronization, see Device Out of Sync Alerts. **Note** If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory. **Note** If you edit the Unified CM Publisher, the Unified CM Subscribers associated with the publisher are updated automatically. You cannot edit Unified CM Subscribers from the System Inventory. **To associate the external HDS with a default Cisco Identity Service (IdS) for single sign-on:** **1.** Click the pencil icon on the external HDS. **2.** Click the Search icon next to **Default Identity Service**. **3.** Enter the machine name for the Cisco IdS in the Search field or choose the Cisco IdS from the list. **4.** Click **Save**. **To delete**, click the **x** on the machine. Confirm the deletion. You can open the administration tool for these external machines by clicking the **arrow** icon in the machine box: • **Unified CM Publisher** • SocialMiner • **MediaSense**

Item	Notes	Actions
	This section shows all external machines in the deployment, and can include any of the following: • HDS • Unified CM Publisher • Unified CM Subscriber • SocialMiner • ECE Data Server (refers to ECE Data Server VM for 400 agents and Services Server VM for ECE 1500 agents) • ECE Web Server • 3rd Party Multichannel • Unified CVP Reporting • MediaSense • Unified SIP Proxy • Virtualized Voice Browser • Gateway • Media Server **Note** • Unified CM Subscriber machines are dedicated to the contact center. When you configure an external Unified CM Publisher, its Unified CM Subscribers are added to the System Inventory automatically.	

Monitor Server Status Rules for Packaged CCE 2000 Agents Deployment

In Packaged CCE 2000 Agents deployment, the Inventory displays the total number of alerts for machines with validation rules. Click the alert count to open the **Server Status** popup window, which lists all of the rules for that machine and indicates which have warnings and errors. Rules are grouped by these categories:

Server Status Category	Description	Example Rules
Configuration	Rules for installation and configuration of a component. These rules identify problems with mismatched configuration between components, missing services, and incorrectly configured services.	**Unified CCE Rogger:** The trace level must be set to normal to ensure performance. **Unified CVP:** The names of the SIP Server Groups on CVP containing Communications Manager addresses must match the Communications Manager Cluster Fully Qualified Domain Name.
Operations	Rules for the runtime status of a component. These rules identify services and processes that cannot be reached, are not running, or are not in the expected state.	**Unified CCE Rogger:** The central controller agent process (ccagent.exe) must be in service for both PGs. **Note** Webex Experience Management and Call Transcript should be reachable on Network.
System Health	Metrics to monitor the CPU, memory, and disk usage of a component's Virtual Machine (VM) as reported by ESXi over the last 10 minutes. The memory and CPU usage may differ slightly from system tools reported by the VM itself. For VM Hosts, these metrics also include datastore performance information. For VM Hosts under M5 Tested Reference Configuration / Specification Based Configuration, these metrics include CPU reservation, CPU oversubscription, memory reservation and datastore utilization information.	**All:** Memory usage as reported by ESXi - 17% For VM Hosts under M5 Tested Reference Configuration / Specification Based Configuration: • Maximum CPU Reservation - 65% • Maximum CPU Oversubscription - 200% • Maximum Memory Reservation - 80% • Maximum Storage Usage per Datastore - 80%
VM	VM requirements for a component.	**All:** VMware Tools must be up to date

Server Status Category	Description	Example Rules
System Validation	Rules for Unified CCE database and configuration settings. These rules identify whether the configuration of objects in your deployment match the requirements and limits for Packaged Contact Center Enterprise. **Note** The System Validation category is available only for the Side A Unified CCE AW-HDS-DDS.	**Side A Unified CCE AW-HDS-DDS:** Agent Desk Settings: Ring No Answer Times must not be set. **Side A Unified CCE AW-HDS-DDS:** Application Gateway **Side A Unified CCE AW-HDS-DDS:** Application Instance: Up to 12 Application Instances can be defined.

VM Validation

The validation for the Packaged CCE: 2000 Agents deployment type makes the following checks to ensure hardware compliance and conformance with the Cisco-provided OVA files.

- For Hosts:
  - BIOS
  - Minimum number of CPU cores
  - Minimum memory
  - Data store size
- For VMs:
  - Number of virtual CPU cores
  - Number of configured networks
  - Virtual network card driver (except for Unified CM)
  - VM is powered on
  - CPU reservation
  - Exact memory
  - Exact disk size
  - Exact number of disks
  - VMware tools

Configure Cisco Unified Contact Center Enterprise PG

The following table outlines the configuration task for Media Routing Peripheral Gateway for the Packaged CCE 2000 Agents deployment.

Configuration Task
Add PIMs to the Media Routing Peripheral Gateway (optional)

Cisco SNMP Setup

Complete the following procedures to configure Cisco SNMP:

- Add Cisco SNMP Agent Management Snap-In, on page 21
- Save Cisco SNMP Agent Management Snap-In View, on page 21
- Set Up Community Names for SNMP V1 and V2c , on page 22
- Set Up SNMP User Names for SNMP V3 , on page 22
- Set Up SNMP Trap Destinations , on page 23
- Set Up SNMP Syslog Destinations , on page 23

Add Cisco SNMP Agent Management Snap-In

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

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

Procedure

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

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

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

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

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

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

Save Cisco SNMP Agent Management Snap-In View

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

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

Procedure

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

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

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

Step 4 Click **Save**.

Set Up Community Names for SNMP V1 and V2c

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

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

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 21 and Save Cisco SNMP Agent Management Snap-In View, on page 21.

Procedure

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

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

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

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

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

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

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

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

Set Up SNMP User Names for SNMP V3

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

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

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 21 and Save Cisco SNMP Agent Management Snap-In View, on page 21.

Procedure

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

Step 2 Click **Add New User**.

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

Step 4 Click **Save**.

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

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

Set Up SNMP Trap Destinations

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

Complete the following procedure to configure the trap destinations.

Before you begin

Ensure Cisco SNMP is added and saved using the procedures Add Cisco SNMP Agent Management Snap-In, on page 21 and Save Cisco SNMP Agent Management Snap-In View, on page 21.

Procedure

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

Step 2 Click **Add Trap Entity**.

Step 3 Click the SNMP version that your NMS uses.

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

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

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

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

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

Step 8 Click **OK**.

Set Up SNMP Syslog Destinations

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

Complete the following procedure to configure Syslog destinations.

Procedure

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

Step 2 Choose an Instance from the list box.

Step 3 Check **Enable Feed**.

Step 4 Enter an IP address or host name in the Collector Address field.

Step 5 Click **Save**.

Step 6 Click **OK** and restart the logger.

Configure Cisco Unified Customer Voice Portal

The following table outlines the Cisco Unified Customer Voice Portal (CVP) configuration tasks for Packaged 2000 Agents deployment.

Note The CVP configurations are site specific. Side A and Side B configurations per site must be the same.

Configuration Tasks
To secure communication between Call Server and ICM, see Secure GED 125 Communication between Call Server and ICM. For more information about securing CVP communication, see Unified CVP Security
For web secure communication, see pcce_b_admin-and-config-guide_120_appendix3.pdf#nameddest=unique_88
To change the default settings, see CVP Server Services Setup
Configure Media Server
Configure SNMP, on page 82

Configure Cisco Unified Communications Manager

The following table outlines the Cisco Unified Communications Manager configuration tasks for Packaged CCE 2000 Agents deployment.

Configuration Tasks
For details on CA and self-signed certificate, see Secure Communication on CUCM
Configure Fully Qualified Domain Name, on page 25
Configure Cisco Unified Communications Manager Groups, on page 25
Configure Conference Bridges, on page 26
Configure Media Termination Points, on page 26
Transcoder Configuration in Unified CM and IOS Gateway, on page 27
Configure Media Resource Groups, on page 27
Configure and Associate Media Resource Group List, on page 28
Configure CTI Route Point, on page 28
Configure Ingress Gateways for Locations-based Call Admission Control, on page 29

Configuration Tasks
Add a SIP Profile in Unified CM, on page 29
Configure Trunk, on page 30
Configure Route Group, on page 30
Configure Route List, on page 31
Configure Route Pattern, on page 31

Configure Fully Qualified Domain Name

Procedure

Step 1 Open Cisco Unified Communications Manager and log in.

Step 2 Navigate to **System** > **Enterprise Parameters**.

Step 3 Fill in **Clusterwide Domain Configuration** > **Cluster Fully Qualified Domain Name** with the Fully Qualified Domain Name of your cluster.

Example:

ccm.hcscc.icm

Note The Cluster Fully Qualified Domain Name is the name of the Unified Communications Manager Server Group defined in Unified CVP.

Step 4 Click **Save**.

Configure Cisco Unified Communications Manager Groups

Complete the following procedure to add a Cisco Unified Communications Manager to the Unified Communications Manager Group.

Procedure

Step 1 Select Cisco Unified CM Administrator from the **Navigation** menu and click **Go**.

Step 2 Select **System > Cisco Unified CM Group**.

Step 3 Click **Find**. Then click **Default**.

Step 4 Move the two subscribers from the Available panel to the Selected panel.

Step 5 Click **Save**.

Step 6 Click **Reset**.

Step 7 On the **Device Reset** popup, click **Reset**.

Step 8 Click **Close**.

Configure Conference Bridges

Perform this procedure for each gateway in the deployment.

Procedure

Step 1 Select **Media Resources** > **Conference bridge**.

Step 2 Click **Add New**.

Step 3 Select Conference Bridge Type of **Cisco IOS Conference Bridge**.

Step 4 In the **Conference Bridge name** field, enter a unique identifier for the conference bridge name that matches the configuration on the gateway.

In the example, this is gw70conf.

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

Step 5 Select a Device Pool.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Configure Media Termination Points

Complete this procedure for each gateway in the deployment.

Procedure

Step 1 Select **Media Resources** > **Media Termination Point**.

Step 2 Click **Add New**.

Step 3 In the Media Termination Point Name field, enter a unique identifier for the media termination that coincides with the configuration on the gateway.

In the example, this is gw70mtp.

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

Step 4 Select a Device Pool.

Step 5 Click **Save**.

Step 6 Click **Apply Config**.

Transcoder Configuration in Unified CM and IOS Gateway

A transcoder is required for multicodec scenarios to convert a stream from a G.711 codec to a G.729 codec.

For more information about transcoder configuration in Unified Communications Manager and gateway, see the section "Configure Transcoders and Media Termination Points" in the *System Configuration Guide for Cisco Unified Communications Manager* at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Configure Transcoders

Perform this procedure for each gateway in the deployment.

Procedure

Step 1 In Unified Communications Manager Administration, select **Media Resources** > **Transcoder.**

Step 2 Click **Add New**.

Step 3 For Transcoder Type, select **Cisco IOS enhanced media termination point**.

Step 4 In the **Device Name** field, enter a unique identifier for the transcoder name that coincides with the configuration on the gateway.

In the following example, this is gw70xcode.

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

Step 5 In the **Device Pool** field, select the appropriate device pool.

Step 6 Click **Save**.

Step 7 Click **Apply Config**.

Configure the CVP Call Server Dial Peers in Ingress Gateway

The Ingress Gateway to Unified CVP outbound dial peer configuration uses the IPv4 address of Unified CVP as the session target.

Configure Media Resource Groups

Procedure

Step 1 Select **Media Resources** > **Media Resource Group**.

Step 2 Add a Media Resource Group for Conference Bridges.

a) Click **Add New**.

b) Enter a Name.

c) From the Available list, select all the Cisco IOS conference bridge resources configured for each ingress/VXML combination gateway in the deployment and add them to the group.

d) Click **Save**.

Step 3 Add a Media Resource Group for Media Termination Point.

a) Click **Add New**.
b) Enter a Name.
c) From the Available list, select all the hardware media termination points configured and add them to the group.
d) Click **Save**.

Step 4 Add a Media Resource Group for Transcoder.

a) Click **Add New**.
b) Enter a Name.
c) From the Available list, select all the transcoders configured and add them to the group.
d) Click **Save**.

Step 5 Click **Save.**

Configure and Associate Media Resource Group List

Procedure

Step 1 Select **Media Resources** > **Media Resource Group List**.

Step 2 Click **Add New** and enter a Name.

Step 3 Add a Media Resource Group list and associate all of the media resource groups. Click **Save**.

Step 4 Select **System** > **Device Pool**. Click **Find**. Select the appropriate device pool.

Step 5 From the Media Resource Group List drop-down list, choose the media resource group list added in Step 2.

Step 6 Click **Save**. Click **Reset**.

Configure CTI Route Point

Complete the following procedure to add a computer telephony integration (CTI) route point for agents to use for transfers and conferences.

Procedure

Step 1 In Cisco Unified CM Administration, select **Device** > **CTI Route Point**.

Step 2 Click **Add New**.

Step 3 Set a device name; for example, **PCCEInternalDNs**.

Step 4 For Device Pool, select **Default**.

Step 5 Select a Media Resource Group List from the list.

Step 6 Click **Save.**

Step 7 Click on Line [1] to configure the directory number associated with this route point.

This directory number will be a pattern that is intended to match any of the internal Dialed Numbers you configure in Packaged CCE for internally routed calls. (For instance, for Transfers and Conferences).

Important Define a pattern that is flexible enough to match all your internal dialed numbers yet restrictive enough not to inadvertently intercept calls intended for other Route Patterns you may have defined for other parts of your dial plan. Use a unique prefix for internal calls. For example, if you have internal dialed numbers 1230000 and 1231111, then an appropriate line number to enter for the cti route point would be 123XXXX.

Step 8 Select **User Management** > **Application User**.

Step 9 Select *pguser* created during Packaged CCE automated initialization.

Step 10 Select the CTI Route Point from the list of **Available Devices**, and add it to the list of **Controlled Devices**.

Step 11 Click **Save.**

Configure Ingress Gateways for Locations-based Call Admission Control

Locations-based call admission control (CAC) is used in the Unified CCE branch-office call flow model (also known as the Centralized Model). This means that all servers (Unified CVP, Unified CCE, Unified Communications Manager, and SIP Proxy server) are centralized in one or two data centers, and each branch office.

Configure Unified Communications Manager to use the Ingress gateway instead of Unified CVP as the originating location of the call. This configuration ensures that CAC can be properly adjusted based on the locations of the calling endpoint and the phone.

Important Do not define Unified CVP as a gateway device in Unified Communications Manager.

Procedure

In Cisco Unified CM Administration, define the Ingress gateways as gateway devices. Assign the correct location to the devices.

Add a SIP Profile in Unified CM

This option allows a dual-stack SIP trunk to offer both IPv4 and IPv6 media. Perform this procedure for IPv6-enabled deployments only.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **SIP Profile**.

Step 2 Click **Add New** and enter the name of the SIP profile.

Step 3 Check the **Enable ANAT** check box on the SIP Profile.

Step 4 Save your changes.

Configure Trunk

There are two Unified CVP Servers and each must be associated with a SIP trunk in Unified Communications Manager. The following procedure explains how to configure the SIP trunks, each targeting a different Unified CVP Server.

Actual site topology may necessitate the use of alternate SIP trunk plans, which are supported as long as both Unified CVP Servers are targeted by the configured SIP trunks.

Procedure

Step 1 In Unified Cisco CM Administration, select **Device** > **Trunk.**

Step 2 Click **Add New**.

Step 3 From the Trunk Type drop-down list, choose **SIP Trunk**, and then click **Next**.

Step 4 Enter the following in the **Device Information** section:

a) In the **Device Name** field, enter a name for the SIP trunk, for example, **`sipTrunkCVPA`**.
b) In the **Device Pool** drop-down list, select the device pool that the customer has defined.
c) Select a Media Resource Group List from the list.
d) Make sure that the **Media Termination Point Required** check box is not checked.

Step 5 Scroll down to the **SIP Information** section:

a) In Row 1 of the **Destination** table, enter the IP address of a CVP server. Accept the default destination port of 5060.
b) In the **SIP Trunk Security Profile** drop-down list, select **Non Secure SIP Trunk Profile**.
c) In the **SIP Profile** drop-down list, select **Standard SIP Profile**.

Note If you are using an IPv6-enabled deployment, use the SIP Profile created in Add a SIP Profile in Unified CM, on page 29.

d) In the **DTMF Signaling Method** drop-down list, select **RFC 2833**.

Step 6 Click **Save**.

Step 7 Click **Reset**.

Step 8 Repeat for all the remaining Unified CVP servers in the deployment.

Configure Route Group

Complete the following procedure to create a route group.

Procedure

Step 1 In Unified Communications Manager, select **Call Routing** > **Route Hunt** > **Route Group**.

Step 2 Click **Add New**.

Step 3 Enter a name for the route group; for example, **CVP Route Group**.

Step 4 Using the Add to Route Group button, add all CVP Trunks as Selected Devices.

Step 5 Click **Save**.

Configure Route List

Complete the following procedure to add a route list to the route group.

Procedure

Step 1 In Unified Communications Manager, select **Call Routing** > **Route Hunt** > **Route List**.

Step 2 Click **Add New**.

Step 3 Enter a name for the route list; for example, **CVP Route List**.

Step 4 Select a Cisco Unified Communications Manager Group.

Step 5 Add the route group you created.

Step 6 Click **Save**.

Configure Route Pattern

Complete the following procedure to add a route pattern to the route list.

Procedure

Step 1 In Unified Communications Manager, select **Call Routing** > **Route Hunt** > **Route Pattern**.

Step 2 Click **Add New**.

Step 3 Enter a route pattern of `8881111000XXXX`.

Step 4 Select the route list that you created.

Step 5 Keep all defaults in all panels

Step 6 Click **Save**.

Step 7 Click **OK** at the message about the Forced Authorization Code. You do not want a Forced Authorization Code.

Configure Cisco Unified Intelligence Center

Follow this sequence to configure the Cisco Unified Intelligence Center for Packaged CCE 2000 Agentsdeployment

Sequence	Task
1	For details on security certificate, see *Cisco Unified Intelligence Center User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html
2	For details on self-signed certificate, see Add IdS Certificate to AW Machine
3	Download Report Bundles, on page 33
4	Import Reports, on page 33
5	Configure Unified Intelligence Center Administration, on page 35

Configure Unified Intelligence Center Data Sources for External HDS

Perform this procedure only if your deployment includes an external HDS and you wish to have a longer retention period.

Before you begin

Configure the Unified Intelligence Center SQL user for the External HDS databases before configuring the data sources (applicable for 4000 Agents and 12000 Agents). For more information, refer the Configure Unified Intelligence Center SQL User Account on the External HDS section in the Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html

Procedure

Step 1 Sign in to Unified Intelligence Center with your Cisco Intelligence Center administrator account (https://<hostname/ IP address of CUIC Publisher>:8444/cuicui).

Step 2 Select **Configure** > **Data Sources**.

Step 3 Click **Data Sources** in the left panel.

Step 4 Select the **UCCE Historical** data source. Click **Edit**.

a) In the **Datasource Host** field, enter the IP Address of the external HDS server.
b) In the **Port** field, enter the AW SQL server port number. The default is `1433`.
c) In the **Database Name** field, enter `{instance}_awdb`.
d) Leave the **Instance** field blank.
e) Select the **Timezone**.
f) In the **Database User ID**, enter the user name that you configured for the Cisco Unified Intelligence Center SQL Server user account.
g) Enter and confirm the SQL Server User **password**.
h) Select the **Charset** based on the collation of SQL Server installation.
i) Click **Test Connection**.
j) Click **Save**.

Step 5 Click the **Secondary** tab to configure Unified CCE Historical Data Source.

a) Check the **Failover Enabled** checkbox.
b) In the **Datasource Host** field, enter the IP address of the second external HDS server.

c) In the **Port** field, enter **`1433`**.

d) In the **Database Name** field, enter **`{instance}_awdb`**.

e) Complete other fields as in the Primary tab.

f) Click **Test Connection**.

g) Click **Save**.

Step 6 Repeat this procedure for the **UCCE Realtime** datasource for 4000 or 12000 Agents deployment.

The **Database Name** for the Realtime Data Source is **`{instance}_awdb`**.

Download Report Bundles

The following Cisco Unified Intelligence Center report bundles are available as downloads from Cisco.com https://software.cisco.com/download/type.html?mdfid=282163829&catid=null. Click the **Intelligence Center Reports** link to view all available report bundles:

- Realtime and Historical Transitional templates - Introductory templates designed for new users. These templates are simplified versions of the All Fields templates, and are similar to templates available in other contact center solutions.

- Realtime and Historical All Fields templates - Templates that provide data from all fields in a database. These templates are most useful as a basis for creating custom report templates.

- Live Data templates - Templates that provide up to the moment data for contact center activity.

- Realtime and Historical Outbound templates - Templates for reporting on Outbound Option activity. Import these templates if your deployment includes Outbound Option.

- Realtime and Historical SocialMiner templates - Templates for reporting on SocialMiner activity. Import these templates if your deployment includes SocialMiner.

- Cisco Unified Intelligence Center Admin Security templates - Templates to report on Cisco Unified Intelligence Server audit trails, permissions, and template ownership.

Some of the templates in these bundles are not applicable in Cisco Packaged CCE deployment. See the *Cisco Packaged Contact Center Enterprise Reporting User Guide* at https://www.cisco.com/en/US/products/ps12586/tsd_products_support_series_home.html for more information about the templates used in Packaged CCE deployments.

Additionally, sample custom report templates are available from Cisco DevNet (https://developer.cisco.com/site/reporting/documentation/) and include templates for:

- Enterprise Chat and Email

- Cisco Unified Customer Voice Portal (Unified CVP)

When downloading report template bundles, select bundles for the version of software deployed in your contact center.

Import Reports

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

The imported report retrieves data for the following entities:

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

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

Note You cannot import Report Filters and Collections.

To import reports, perform the following steps:

Procedure

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

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

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

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

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

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

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

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

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

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

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

Step 9 Select the files to import or overwrite.

- Overwrite—If the report being imported exists in the Unified Intelligence Center.

- Import—If the report being imported is the new set of report files.

Step 10 Click **Import**.

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

Configure Unified Intelligence Center Administration

Procedure

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

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

a) Enter the Host Address for the Primary Active Directory Server.
b) Leave the default value for Port.
c) Complete the **Manager Distinguished Name** fields.
d) Enter and confirm the password with which the Manager accesses the domain controller.
e) For User Search Base, specify the Distinguished Name or Organization Unit of the domain you want to search.
f) For Attribute for User ID, select the required option.

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

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

Note For more details, see the online help.

Step 3 Configure syslog for all devices.

a) Choose **Device Management** > **Logs and Traces Settings**.
b) For each host address:

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

Step 4 Configure SNMP for all devices, if used.

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

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

- V1/V2c Community Strings.
- Notification Destination.

Configure Cisco Finesse

Follow this sequence to configure the Cisco Finesse for Packaged CCE 2000 Agents deployment

Sequence	Task
1	For details on CA certificate, see *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html
2	For details on self-signed certificate, see Add Finesse Certificate to AW Machine
3	Configure Contact Center Agents and Routing for Live Data Reports, on page 36
4	Live Data Reports, on page 36

Configure Contact Center Agents and Routing for Live Data Reports

In order to test the Live Data reports in the Finesse desktops, configure the following in Unified CCE Administration(`https://<Side A/B Unified CCE AW-HDS-DDS IP address>/cceadmin`):

- Agents
- Skill groups or precision queues
- Call types
- Dialed numbers
- Network VRU scripts
- Routing scripts

Note Routing scripts are configured in Script Editor, which you can open from Unified CCE Administration Tools.

Live Data Reports

Cisco Unified Intelligence Center provides Live Data real-time reports that you can add to the Finesse desktop.

Add Live Data Reports to Finesse

The following sections describe how to add the Live Data reports to the Finesse desktop. The procedure that you follow depends on several factors, described in the following table.

Procedure	When to use
Add Live Data reports to default desktop layout	Use this procedure if you want to add Live Data reports to the Finesse desktop after a fresh installation or after an upgrade if you have not customized the default desktop layout.
Add Live Data reports to custom desktop layout	Use this procedure if you have customized the Finesse desktop layout.
Add Live Data reports to team layout	Use this procedure if you want to add Live Data reports to the desktop layout for specific teams only.

Add Live Data Reports to Default Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to the default desktop layout. Use this procedure after a fresh installation of Finesse. If you upgraded Finesse but do not have a custom desktop layout, click **Restore Default Layout** on the Manage Desktop Layout gadget and then follow the steps in this procedure. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Desktop** > **Resources**.

Step 2 Click the **Desktop Layout** tab.

Step 3 Remove the comment characters (<!-- and -->) from each report that you want to add to the desktop layout. Make sure you choose the reports that match the method your agents use to access the Finesse desktop (HTTP or HTTPS).

Step 4 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 5 Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows, replacing 310 with 400:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 6 Click **Save**.

Add Live Data Reports to Custom Desktop Layout

The Finesse default layout XML contains commented XML code for the Live Data report gadgets available for the Finesse desktop. The gadgets are divided into two categories: HTTPS version of Live Data gadgets and HTTP version of Live Data gadgets.

This procedure explains how to add the Live Data report gadgets to a custom desktop layout. Note that line breaks and spaces that appear in the example text are provided only for readability and must not be included in the actual code.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Desktop** > **Resources**.

Step 2 Click the **Desktop Layout** tab.

Step 3 Click **Finesse Default Layout XML** to show the default layout XML.

Step 4 Copy the XML code for the report you want to add from the Finesse default layout XML.

Example:

To add the Agent Report for HTTPS, copy the following:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&
        viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
</gadget>
```

Step 5 Paste the XML within the tab tags where you want it to appear.

Example:

To add the report to the home tab of the agent desktop:

```
<layout>
  <role>Agent</role>
  <page>
    <gadget>/desktop/gadgets/CallControl.jsp</gadget>
  </page>
  <tabs>
    <tab>
      <id>home</id>
      <label>finesse.container.tabs.agent.homeLabel</label>
      <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
              gadgetHeight=310&viewId_1=99E6C8E210000141000000D80A0006C4&
              filterId_1=agent.id=CL%20teamName&
              viewId_2=9AB7848B10000141000001C50A0006C4&
              filterId_2=agent.id=CL%20teamName
      </gadget>
    </tab>
    <tab>
      <id>manageCall</id>
```

```
   <label>finesse.container.tabs.agent.manageCallLabel</label>
  </tab>
 </tabs>
</layout>
```

Step 6 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 7 Optionally, change the gadget height.

Example:

The height specified in the Live Data gadget URLs is 310 pixels. If you want to change the height, change the gadgetHeight parameter in the URL to the desired value. For example, if you want the gadget height to be 400 pixels, change the code as follows:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
    gadgetHeight=400&viewId_1=99E6C8E210000141000000D80A0006C4&
    filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
    filterId_2=agent.id=CL%20teamName
    </gadget>
```

To maintain the optimal display of the gadget with scroll bars, set the value for the gadget height to a minimum of 200 pixels. If the report does not require scroll bars, for example a one-row report, you can set a smaller gadget height (for example, 100 pixels). If you do not specify anything for the gadget height (if you remove the 310 from the URL), it defaults to 170 pixels.

Step 8 Click **Save**.

Note After you add a gadget, sign in to the Finesse desktop and make sure it appears the way you want. If you use a report with a large number of rows, you may want to adjust the gadget height or the screen resolution on the computer used to access the desktop to make the report easier to read or make more rows appear on the screen without needing to scroll down.

Agents who are signed in when you change the desktop layout must sign out and sign back in to see the change on their desktops.

Configure Cisco Unified Customer Voice Portal Reporting Server

Follow this sequence to configure the Cisco Unified Customer Voice Portal Reporting Server for Packaged CCE deployment

Note The Unified CVP Reporting VM is required for customers who use Courtesy Callback and who want to run Unified CVP call and application reports.

Sequence	Task
1	Import WSM CA Certificate into CVP
2	For details on self-signed, see Import WSM Certificate into AW Machines
3	Obtain Cisco Unified Customer Voice Portal Report Templates, on page 40
4	Create Data Source for Cisco Unified CVP Report Data, on page 40

Sequence	Task
5	Import Unified CVP Report Templates in Unified Intelligence Center, on page 42

Obtain Cisco Unified Customer Voice Portal Report Templates

To import Unified CVP report templates complete the following:

Procedure

Step 1 On the Unified CVP Reporting Server, click **Start**.

Step 2 In the search box, type **%CVP_HOME%\CVP_Reporting_Templates** and press **Enter**.

Step 3 Compress the reports into a zip folder and copy it to the system from which you will run Unified Intelligence Center Administration.

Create Data Source for Cisco Unified CVP Report Data

Perform the following procedure to create a data source.

Procedure

Step 1 Log in to the Unified Intelligence Center at `https://`*`<hostname/ IP address of CUIC Publisher>`*`:8444/cuicui`.

Step 2 Select the **Data Sources** drawer to open the **Data Sources** page.

Step 3 Click **New** to open **New Data Source** page.

Step 4 Complete fields on this page as follows:

Field	Value
Name	Enter the name of this data source. Report Designers and Report Definition Designers do not have access to the Data Sources page but can see the list of Data Sources when they create custom reports. To benefit those users, give a new Data Source a meaningful name.
Description	Enter a description for this data source.
Data Source Type	Choose **Informix**. **Note** Type is disabled in Edit mode.
Host Settings	
Database Host	Enter the IP address or hostname for the Unified CVP Reporting server.

Field	Value
Port	Enter the port number. Typically, the port is 1526. You may have to open this port in the CVP Reporting Server firewall (Windows Firewall > Advanced Settings > Inbound rules > new rule).
Database Name	Enter the name of the reporting database on the Unified CVP reporting server. The database name can be `cvp_data` or `callback`.
Instance	Specify the instance name of the desired database. By default, this is `cvp`.
Timezone	Choose the correct time zone for the data stored in the database. In locations that change from Standard Time to Daylight Savings Time, this time zone is updated automatically. **Note** Set CVP datasource timezone configuration to UTC on CUIC.
Authentication Settings	
Database User ID	Enter the user ID of the Reporting User to access the Unified CVP reporting database. (The cvp_dbuser account is created automatically during Unified CVP Reporting server installation.)
Password and Confirm Password	Enter and confirm the password for the database user.
Charset	Choose UTF-8.
Default Permissions	View or edit the permissions for this datasource for My Group and for the All Users group.
Max Pool Size	Select the maximum pool size. Value ranges from 5-200. The default Max Pool Size value is 100 and is common for both the primary and secondary data source tabs.

Step 5 Click **Test Connection**.

If the status is not Online, review the error message to determine the cause and edit the data source accordingly.

Step 6 Click **Save** to close the Add Data Source window.

The new data source appears on the Data Sources list.

Import Unified CVP Report Templates in Unified Intelligence Center

You can import a report (XML) and the associated template help file (ZIP format) into Cisco Unified Intelligence Center.

Procedure

Step 1 Launch the Unified Intelligence Center web application at `https://<Hostname/IP Address of CUIC Publisher>:8444/cuic`

Step 2 From the left navigation pane, click **Reports**.

Step 3 On the Reports toolbar, click **New** > **Import**.
You will be redirected to the legacy interface.

Step 4 Navigate to the folder where you want to import the report.

Note If you are importing a stock report bundle from Cisco.com, it must be placed at the Reports folder level.

Step 5 Click **Import Report**.

Step 6 In the **File Name (XML or ZIP file)** field, click **Choose File**.

Step 7 Browse to and select the XML or the compressed report file, and click **Open**.

Step 8 From the **Data source for ReportDefinition** drop-down list, select a data source used by the report definition.

Note This field appears only if the Report Definition for the report being imported is not currently defined in Unified Intelligence Center.

Step 9 From the **Data Source for ValueList** drop-down list, select the data source used by the value lists defined in the report definition.

Note You have to select a data source for the value list only if it does not use the same data source as the Report Definition. For Report Definitions of Real Time Streaming, it is mandatory to select a data source for the Value Lists.

Step 10 In the **Save To** field, browse to the folder where you want to place the imported report. Use the arrow keys to expand the folders.

Step 11 Click **Import**.

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

Configure VVB

Note
- If you have configured VXML Gateway, it is not mandatory to configure Virtualized Voice Browser (VVB). You may configure either VVB or VXML Gateway, or configure both.
- The Cisco VVB configurations are site specific. All the VVBs in a site must have the same configurations.

To configure Cisco VVB for all deployments:

- Add VVB as an external machine. For more information, see Add External Machines.
- Change the default configuration (Optional). For more information, see Cisco Virtualized Voice Browser (VVB) Setup.
- Configure SNMP (Optional). For more information, see Configure SNMP, on page 87.

Configure Cisco IOS Enterprise Voice Gateway

Tasks to configure the Cisco IOS Enterprise Voice Gateway for Packaged CCE deployment

Task
Common Configuration for the Ingress Gateway and VXML Gateway, on page 43
Configure Ingress Gateway, on page 44
Configure VXML Gateway, on page 47 (optional)
Configure Codec for Ingress and VXML Gateways, on page 49

About Ingress and VXML Gateway Configuration

Complete the following procedures to configure the Ingress Gateway and VXML Gateway. Instructions are applicable to both TDM and Cisco Unified Border Element (CUBE) Voice gateways, unless otherwise noted.

You can add all Gateways as an external machine. For more information, see Add External Machines.

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

Common Configuration for the Ingress Gateway and VXML Gateway

```
logging buffered 2000000 debugging
no logging console
service timestamps debug datetime msec localtime
ip routing
ip cef
ip source-route
interface GigabitEthernet0/0
```

```
     ip route-cache same-interface
     duplex auto
     speed auto
     no keepalive
     no cdp enable

voice service voip
          ip address trusted list
          ipv4 0.0.0.0 0.0.0.0 # OR an explicit Source IP Address Trust List
     allow-connections sip to sip
     signaling forward unconditional
```

Configure Ingress Gateway

Procedure

Step 1 Configure global settings.

```
voice service voip
  allow-connections sip to sip
 signaling forward unconditional
 # If this gateway is being licensed as a Cisco UBE the following lines are also required
 mode border-element
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0               # Or an explicit Source IP Address Trust List
sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

Step 2 Configure voice codec preference:

```
voice class codec 1
     codec preference 1 g711ulaw
     codec preference 2 g711alaw
     codec preference 3 g729r8
```

Step 3 Configure default services:

To download and transfer the `survivability.tcl` file to the Ingress Gateway, see File Transfer to Gateway, on page 49.

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

Step 4 Configure gateway and sip-ua timers:

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

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

Step 5 Configure POTS dial-peers:

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

Note This is required for TDM gateways only.

Step 6 Configure the switch leg:

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

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

dial-peer voice 70022 voip
     description Used for Switch leg SIP Direct
     preference 2
     max-conn 225
     destination-pattern xxxx...... #Customer specific destination pattern
     session protocol sipv2
     session target ipv4:###.###.###.###    #IP Address for Unified CVP, SideB
     session transport tcp
     voice-class codec 1
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     no vad
```

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

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

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

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

```
voice-card 3
     dspfarm
     dsp services dspfarm
voice-card 4
     dspfarm
     dsp services dspfarm

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

# Add a SCCP group for each of the hardware resource types
sccp ccm group 1
     associate ccm 1 priority 1
     associate profile 2 register <gatewaynamemtp>
     associate profile 1 register <gatewaynameconf>
     associate profile 3 register <gatewaynamexcode>

# Configure DSPFarms for Conference, MTP and Transcoder

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

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

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

Step 8 Optional, configure the SIP Trunking:

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

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

Step 9 Configure incoming PSTN SIP trunk dial peer:

```
dial-peer voice 70000 voip
     description Incoming Call From PSTN SIP Trunk
     service survivability
```

```
incoming called-number xxxx……    # Customer specific incoming called-number pattern
voice-class sip rel1xx disable
dtmf-relay rtp-nte
session protocol sipv2
voice-class codec 1
no vad
```

Note This is required for CUBE only.

Configure VXML Gateway

Before you begin

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

Procedure

Step 1 Configure global settings:

```
voice service voip
  allow-connections sip to sip
 signaling forward unconditional
 # If this gateway is being licensed as a Cisco UBE the following lines are also required
 mode border-element
 ip address trusted list
  ipv4 0.0.0.0 0.0.0.0               # Or an explicit Source IP Address Trust List
sip
  rel1xx disable
  header-passing
  options-ping 60
  midcall-signaling passthru
```

Step 2 Configure default Unified CVP services:

To download and transfer the following files to VXML Gateway, see File Transfer to Gateway, on page 49.

```
#Default Unified CVP Services
application
     service new-call flash:bootstrap.vxml
     service CVPSelfService flash:CVPSelfServiceBootstrap.vxml
     service ringtone flash:ringtone.tcl
     service cvperror flash:cvperror.tcl
     service bootstrap flash:bootstrap.tcl
     service handoff flash:handoff.tcl
```

Step 3 Configure dial-peers:

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

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

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

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

```
http client cache memory pool 15000
http client cache memory file 1000
http client cache refresh 864000
no http client connection persistent
http client connection timeout 60
http client connection idle timeout 10
http client response timeout 30
ivr prompt memory 15000

vxml tree memory 500
vxml audioerror
vxml version 2.0
```

Step 5 Configure VXML leg where the incoming called-number matches the Network VRU Label:

```
dial-peer voice 7777 voip
     description Used for VRU leg
     service bootstrap
     incoming called-number 777T
     dtmf-relay rtp-nte
     codec g711ulaw
     no vad
```

Step 6 Exit configuration mode and use the Cisco IOS CLI command **call application voice load <service_Name>** to load the transferred Unified CVP files into the Cisco IOS memory for each Unified CVP service:

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

File Transfer to Gateway

This procedure explains how to download and transfer files to the Gateway.

Procedure

Step 1 Download the `GWDownloads_12.0.zip` from https://software.cisco.com/download/home/270563413/type/280840592/release/12.0(1) and extract it.

Step 2 Fetch the required `.tcl` files and save it to a location in any server.

Step 3 Transfer the `.tcl` files to the flash memory of the Gateway using FTP.

Configure Codec for Ingress and VXML Gateways

Configure Ingress Gateway

Procedure

Step 1 Add the voice class codec 1 to set the codec preference in dial-peer:

Example:

```
voice class codec 1
     codec preference 1 g729r8
     codec preference 2 g711alaw
     codec preference 3 g711ulaw
```

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

Step 2 Modify the dial-peer to specify the codec explicitly for a dial-peer:

```
dial-peer voice 9 voip
     description For Outbound Call for Customer
     destination-pattern <Customer Phone Number Pattern>
     session protocol sipv2
     session target ipv4:<Customer SIP Cloud IP Address>
     session transport tcp
     voice-class sip rel1xx supported "100rel"
     voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 10 voip
     description ***To CUCM Agent Extension For Outbound***
     destination-pattern <Agent Extension Pattern to CUCM>
     session protocol sipv2
     session target ipv4:<CUCM IP Address>
     voice-class sip rel1xx supported "100rel"
     dtmf-relay rtp-nte
     codec g711alaw
```

Configure VXML Gateway

Procedure

Modify the following dial-peer to specify the codec explicitly for a dial-peer:

```
dial-peer voice 919191 voip
     description Unified CVP SIP ringtone dial-peer
     service ringtone
     incoming called-number 9191T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 929292 voip
     description CVP SIP error dial-peer
     service cvperror
     incoming called-number 9292T
     voice-class sip rel1xx disable
     dtmf-relay rtp-nte
     codec g711alaw
     no vad

dial-peer voice 7777 voip
     description Used for VRU leg #Configure VXML leg where the incoming called
     service bootstrap
     incoming called-number 7777T
     dtmf-relay rtp-nte
     codec g711alaw
     no vad
```

Configure IPv6

Tasks to configure IPv6 for Packaged CCE deployment

Task
Set Up IPv6 for VOS-Based Contact Center Applications, on page 51
Configure NAT64 for IPv6-Enabled Deployment, on page 52
Configure IPv6 on Unified CVP Call Server, on page 54
Configure Gateways to Support IPv6, on page 55

Task
Configure IPv6 on Unified Communications Manager, on page 56

IPv6 Configuration

Packaged CCE can support IPv6 connections for agent and supervisor Finesse desktops and phones. An IPv6-enabled deployment can use either all IPv6 endpoints or a mix of IPv4 and IPv6 endpoints. Servers that communicate with these endpoints can accept both IPv4 and IPv6 connections. Communication between servers continues to use IPv4 connections.

This chapter contains the configuration procedures that you perform for IPv6-enabled deployments.

Set Up IPv6 for VOS-Based Contact Center Applications

By default, only IPv4 is enabled for Unified Communications Manager, Cisco Finesse, and Unified Intelligence Center.

If you choose to enable IPv6 on these applications, you must enable it on both the publisher/primary nodes and subscriber/secondary nodes for those applications.

You can use Cisco Unified Operating System Administration or the CLI to enable IPv6.

See the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html for more information about IPv6 support in Packaged CCE deployments.

Set Up IPv6 Using Cisco Unified Operating System Administration

To set up IPv6 using Cisco Unified Operating System Administration, perform the following procedure on the primary and secondary VOS servers.

Procedure

Step 1 Sign into Cisco Unified Operating System Administration on the Publisher/Primary node:.

- Unified Communications Manager and Unified Intelligence Center: `https://`*`<host or IP address of the Publisher or Primary node>`*`/cmplatform`
- Finesse: `https://`*`FQDN of the Primary node`*`:8443/cmplatform`

Step 2 Navigate to **Settings** > **IP** > **Ethernet IPv6**.

Step 3 Check the **Enable IPv6** check box.

Step 4 Enter values for **IPv6Address**, **Prefix Length**, and **Default Gateway**.

Step 5 Check the **Update with Reboot** check box.

Step 6 Click **Save**.
The server restarts.

Step 7 Repeat this procedure on the subscriber/secondary node.

Set Up IPv6 for VOS-Based Applications Using the CLI

To set up IPv6 using the CLI, perform the following procedure on both the primary and secondary VOS servers.

Procedure

Step 1 Access the CLI on the VOS server.

Step 2 To enable or disable IPv6, enter:

set network ipv6 service {enable | disable}

Step 3 Set the IPv6 address and prefix length:

set network ipv6 static_address *addr mask*

Example:

```
set network ipv6 static_address 2001:db8:2::a 64
```

Step 4 Set the default gateway:

set network ipv6 gateway *addr*

Step 5 Restart the system for the changes to take effect.

utils system restart

Step 6 To display the IPv6 settings, enter:

show network ipv6 settings

Configure NAT64 for IPv6-Enabled Deployment

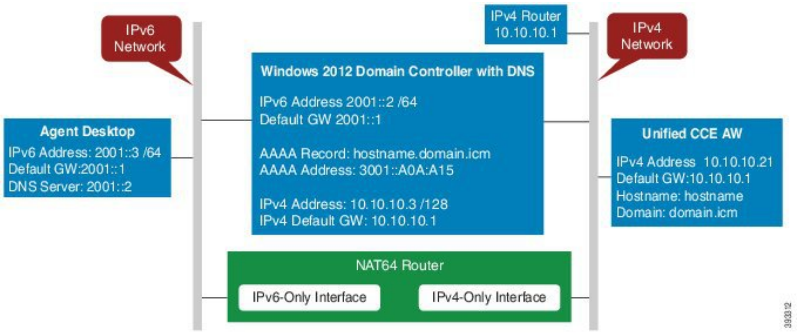
NAT64 allows communication between IPv6 and IPv4 networks. For IPv6-enabled deployments, you must set up NAT64 so that supervisors on an IPv6 network can access Unified CCE Administration web tools on an IPv4 network. You can use either Stateful and Stateless NAT64.

To read more about which translation type is the most appropriate for your deployment see Table 2. Comparison Between Stateless and Stateful NAT64 here: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

Note NAT64 is NOT supported on M train IOS. T train is required.

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

The following example network diagram and interface configuration demonstrates Stateful NAT64 translation between an IPv6 network and an IPv4 network.



```
interface GigabitEthernet0/0
description ipv4-only interface
 ip address 10.10.10.81 255.255.255.128
 duplex auto
 speed auto
 nat64 enable
 no mop enabled

interface GigabitEthernet0/1
description ipv6-only interface
 no ip address
 duplex auto
 speed auto
 nat64 enable
 ipv6 address 2001::1/64
 ipv6 enable

ipv6 unicast-routing
ipv6 cef
!
nat64 prefix stateful 3001::/96
nat64 v4 pool POOL1 10.10.10.129 10.10.10.250
nat64 v6v4 list V6ACL1 pool POOL1 overload
ipv6 router rip RIPv6
!
ipv6 router rip RIP

!
ipv6 access-list V6ACL1
 permit ipv6 2001::/64 any
```

Configure DNS for IPv6

To meet the requirement that Unified CCE Administration be accessed by FQDN, a Forward lookup AAAA record for the Unified CCE AW-HDS-DDS servers and any External HDS servers must be created in DNS.

The steps in this procedure are for a Windows DNS server.

Procedure

Step 1 In Windows, navigate to **Administrative Tools** > **DNS**. This opens the DNS Manager.

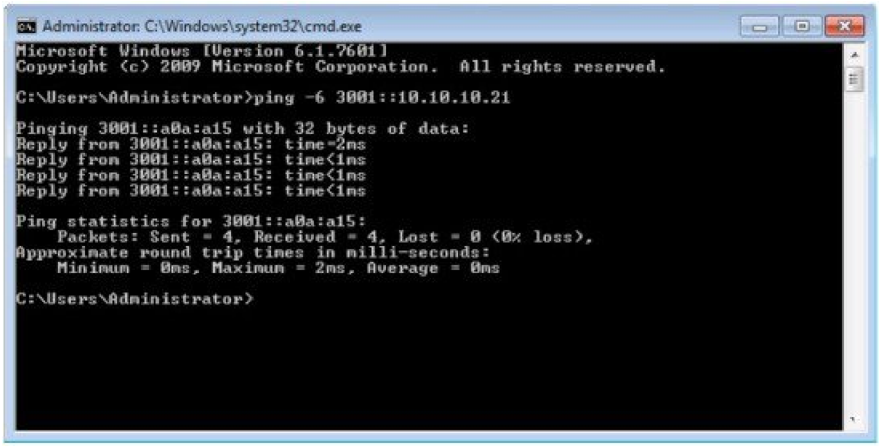
Step 2 In the Forward lookup zone, navigate to your deployment's domain name.

Step 3 Right-click the domain name and select **New Host (A or AAAA)**.

Step 4 In the New Host dialog box, enter the computer name and IP address of the Unified CCE AW-HDS-DDS servers and any External HDS servers. Click **Add Host**.

Determine IPv6 Translation of IPv4 Address for DNS Entry

You can determine the IPv6 address needed for the AAAA DNS record by running a ping command on any Windows machine using mixed notation. Type "ping -6" followed by your IPv6 Nat64 Prefix, two colons, and then the IPv4 address.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ping -6 3001::10.10.10.21

Pinging 3001::a0a:a15 with 32 bytes of data:
Reply from 3001::a0a:a15: time=2ms
Reply from 3001::a0a:a15: time<1ms
Reply from 3001::a0a:a15: time<1ms
Reply from 3001::a0a:a15: time<1ms

Ping statistics for 3001::a0a:a15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\Administrator>
```

In the ping response, the IPv4 address is converted to the hexadecimal equivalent. Use this address in your static AAAA record.

Note Optionally, DNS64 can be used in place of static DNS entries. Use of DNS64 helps facilitate translation between IPv6 and IPv4 networks by synthesizing AAAA resource records from A resource records.

The *NAT64 Technology: Connecting IPv6 and IPv4 Networks* technical paper gives an overview of DNS64 and how it is used with IPv6: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html.

Configure IPv6 on Unified CVP Call Server

For IPv6-enabled deployments, you must add an IPv6 address to your Unified CVP Call Server's existing network interface.

Perform this procedure only if you have an IPv6-enabled environment.

Procedure

Step 1 On the Unified CVP Call Server, navigate to **Control Panel** > **Network and Sharing**.

Step 2 Click **Ethernet**.

Step 3 From the **Ethernet Status** window, select **Properties**.

Step 4 Check the **Internet Protocol Version 6 (TCP/IPv6)** check box, and choose **Properties**.

Step 5 Choose **Use the following IPv6 address** radio button.

Step 6 Enter values in the **IPv6 address**, **Subnet prefix length**, and **Default gateway** fields.

Step 7 Click **OK** and restart Windows when prompted.

Configure Gateways to Support IPv6

For IPv6-enabled deployments, you must configure your Ingress and VXML gateways to enable IPv6 addressing.

Configure an Interface to Support IPv6 Protocol Stack

This procedure applies to both the Ingress and the VXML gateway.

Procedure

Configure the following on the Gateway:

```
>Enable
>configure terminal
>interface type number
>ipv6 address{ ipv6-address / prefix-length | prefix-name sub-bits / prefix-length}
>ipv6 enable
```

Enable ANAT in Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
>voice service voip
>SIP
>ANAT
>bind control source-interface GigabitEthernet0/2
>bind media source-interface GigabitEthernet0/2
```

Enable Dual Stack in the Ingress Gateway

Procedure

Configure the following on the Gateway:

```
>conf t
```

```
>sip-ua
>protocol mode dual-stack preference ipv6
```

Configure IPv6 on Unified Communications Manager

In an IPv6-enabled environment, you must perform the procedures in this section to configure IPv6 on Unified Communications Manager.

Cluster-Wide Configuration in Unified CM Administration

Perform the following procedure to set IPv6 as the addressing mode preference for media and signaling cluster-wide.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **System** > **Enterprise Parameters** > **IPv6 Configuration Modes** to configure the cluster-wide IPv6 settings for each Unified Communications Manager server.

Step 2 From the **Enable IPv6** drop-down list, choose **True**.

Step 3 From the **IP Addressing Mode Preference for Media** drop-down list, choose **IPv6**.

Step 4 From the **IP Addressing Mode Preference for Signaling** drop-down list, choose **IPv6**.

Step 5 From the **Allow Auto-configuration for Phones** drop-down list, choose **Off**.

Step 6 Save your changes.

Transcoding

In an IPv6-enabled environment, a transcoder is required for the following scenarios:

- An agent logged in to an IPv6 endpoint needs to send or receive transfers from an agent logged in to an IPv4 endpoint.
- An agent logged in to an IPv6 endpoint needs to connect to a VXML Gateway for self service.

Add a Common Device Configuration Profile in Unified Communications Manager

In an IPv6-enabled environment, you may have both IPv4 and IPv6 devices.

Perform the following procedure to add an IPv4, IPv6, or dual stack common device configuration profile in Unified Communications Manager.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Device Settings** > **Common Device Configuration**.

Step 2 Click **Add New** and enter the name of the new common device configuration profile.

Step 3 From the **IP Addressing Mode** drop-down list:

- To add an IPv6 common device configuration profile in Unified Communications Manager, choose **IPv6 only**.
- To add an IPv4 common device configuration profile in Unified Communications Manager, choose **IPv4 only**.
- To add a dual stack common device configuration profile in Unified Communications Manager, choose **IPv4 and IPv6**. Then choose **IPv4** from the **IP Addressing Mode Preference for Signaling** drop-down list.

Step 4 Save your changes.

Associate the Common Device Configuration Profile with Gateway Trunk

Perform the following procedure to associate the common device configuration profile with the Gateway trunk. This procedure applies to the Ingress Gateway.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list:

- To associate the IPv6 common device configuration profile with the Gateway trunk, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile with the Gateway trunk, choose the IPv4 common device configuration profile.

Note Unified CM gateway trunk supports only an IPv4 or IPv6 trunk. You cannot associate a dual stack common device configuration profile to a Unified CM gateway trunk.

Step 4 Enter the IPv6 address in the **Destination Address IPv6** field.

Note Unified CM to Gateway trunk supports only standard SIP Profile and does not support ANAT enabled dual-stack SIP trunk.

Step 5 Save your changes.

Associate the Common Device Configuration Profile with an IPv4 or IPv6 Phone

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Phone**.

Step 2 Click **Find**.
Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list: choose the IPv6 common device configuration profile.

- To associate the IPv6 common device configuration profile to an IPv6 phone, choose the IPv6 common device configuration profile.
- To associate the IPv4 common device configuration profile to an IPv4 phone, choose the IPv4 common device configuration profle.

Step 4 Save your changes.

Associate a SIP Profile in Unified CM

In an IPv6-enabled deployment, you must associate a SIP profile with the trunk you configured for Unified CVP.

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**. Choose the trunk profile that you want to view.

Step 3 From the **SIP Profile** drop-down list, choose the SIP Profile you created.

Note For more information on how to create a SIP Profile, see

Add a SIP Profile in Unified CM section in the Cisco Packaged Contact Center Enterprise Administration and Configuration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Step 4 Save your change.

Associate the Dual Stack Common Device Configuration Profile with SIP Trunk

Procedure

Step 1 From **Cisco Unified CM Administration**, choose **Device** > **Trunk**.

Step 2 Click **Find**. Choose the trunk profile that you want to view.

Step 3 From the **Common Device Configuration** drop-down list, choose the Dual Stack Common Device Configuration Profile.

Note For more information on how to add a Dual Stack Common Device Configuration Profile, see Add a Common Device Configuration Profile in Unified Communications Manager, on page 56.

Step 4 Save your change.

Packaged CCE 4000 Agents Deployment

Follow this sequence to configure components for Packaged CCE 4000 Agents deployment.

Sequence	Task
1	Configure CCE Component, on page 59
2	Configure Cisco Unified Customer Voice Portal, on page 81
3	If Media Server is external, Configure Media Server
4	Configure Cisco Unified Communications Manager, on page 85
5	Configure Cisco Unified Intelligence Center, on page 89
6	Configure Cisco Finesse, on page 90
7	Configure Live Data, on page 98
8	Configure Cisco Identity Service, on page 101
9	Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39 (optional)
10	Configure VVB, on page 43 (optional)
11	Configure Cisco IOS Enterprise Voice Gateway, on page 43
12	Configure IPv6, on page 50
13	Configure Enterprise Chat and Email (ECE) (optional) Email and Chat

Configure CCE Component

Follow this sequence to configure components for Packaged CCE 4000 Agents deployment.

Sequence	Task
1	Configure SQL Server for CCE Components, on page 2
2	Set up Organizational Units, on page 2
3	Configure Rogger, on page 60
4	Configure AW-HDS-DDS, on page 64
5	Start Unified CCE Services, on page 64
6	If you have PG VMs installed, Add Unified CCE Instance, on page 76 on all PG VMs
7	Configure Packaged CCE Deployment Type, on page 67
8	Configure Cisco Unified Contact Center Enterprise PG, on page 77

Sequence	Task
9	For configuration using Configuration Manager, see Packaged CCE 4000 and 12000 Agent Supported Tools
10	For details on CA certificate, see Generate and Import CA Signed Certificate in AW Machine
11	For details on self-signed certificate, see Generate and Import Self-signed Certificate in AW Machine

Configure Rogger

Follow this sequence to configure Rogger for Packaged CCE 4000 Agents deployment.

Sequence	Task
1	Add Unified CCE Instance, on page 76
2	Create Logger Database, on page 60
3	To use Outbound Option, see Create Outbound Option Database, on page 61
4	Add Logger Component to Instance, on page 62
5	Add Router Component to Instance, on page 63
6	Cisco SNMP Setup, on page 21 (optional)

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 You can use the Database Size Estimator Tool only after the database is created.

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 Outbound Option Database

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

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**. Right-click the instance name and select **Database** > **Create**.

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

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

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

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

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

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

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

Add Logger Component to Instance

Perform this procedure on the Side A and Side B Loggers.

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 the **Router Private Interface** and **Logger Private Interface**. Then, click **Next**.

Step 5 Check **Enable Historical/Detail Data Replication**.

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

Step 7 Click the **Enable Outbound Option** check box.

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 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 9 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 10 Click **Next**.

Step 11 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 12 Click **Next**.

Step 13 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 14 Accept the default **Automatic Purge at Percent Full**.

Step 15 Click **Next**.

Step 16 In the **Summary** window select the **Create Service Account** option, complete the following steps:

a) Enter the domain user.

Verify that the user is created in the specified domain.

b) Enter the valid password.

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

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

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** .

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 Leave the **Enable Peripheral Gateways** field blank, and click **Next**.

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 Packaged Contact Center Enterprise*, at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-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**.

Start Unified CCE Services

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

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

Procedure

Step 1 On eachUnified CCE Server machine, open **Unified CCE Service Control**.

Step 2 Start the **Unified CCE component** services.

Configure AW-HDS-DDS

Follow this sequence to configure AW-HDS-DDS for Packaged CCE 4000 Agents deployment.

Sequence	Task
1	Configure SQL Server for CCE Components, on page 2
2	Add Unified CCE Instance, on page 76
3	Create HDS Database, on page 64
4	Add Administration and Data Server Component to Instance, on page 65
5	Configure ICM Database Lookup, on page 114 (optional)
6	Cisco SNMP Setup, on page 21 (optional)

Create HDS Database

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

Procedure

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

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

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

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

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

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

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

Step 8 Create the HDS database as follows:

a) From the DB Type drop-down list, choose **HDS**.
b) Click **Add**.
c) On the Add Device dialog box, select **Data**.
d) From the Available Drives list, choose the drive on which you want to install the database.
e) In the Size field, you can leave the default value or enter an appropriate size for your deployment.

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

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

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

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

Add Administration and Data Server Component to Instance

Procedure

Step 1 Open the Web Setup tool.

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

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

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

a) Click **Enterprise**.
b) Select the deployment size:
c) Click **Next**.

Step 5 Select the radio button for your deployment size (either Small to Medium or Large).

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

Step 6 Click **Next**.

Step 7 In a Small to Medium Deployment page, 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 8 Click **Next**.

Step 9 On the Server Role in a Large Deployment page, 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 10 Click **Next**.

Step 11 On the next page of the wizard, 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 their 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 12 On the Database and Options page, configure as follows:

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

Step 13 On the Central Controller Connectivity page, configure as follows:

Note For Packaged CCE 4000 Agents deployment, the IP address of Router and Logger is same.

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 Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html.
g) Click **Next**.

Step 14 In the **Summary** window select the Create Service Account option, and complete the following steps:

a) Create a domain user account. Enter the created domain user.
b) Enter the valid password.
c) Review the Summary and click **Finish**.

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

Configure Packaged CCE Deployment Type

When you configure the Packaged CCE 4000 Agents and 12000 Agents deployment types, you must add a main site. A main or remote site can have zero or more peripheral sets associated with it. Peripheral set is a collection of all components (like Finesse, CVP, and so on) that are dependent on peripheral gateway (including the peripheral gateway itself). For information on how to add peripheral sets, see Add and Maintain Peripheral Set.

Add and Maintain Main Site in 4000 Agents or 12000 Agents Deployment Type

Procedure

Step 1 Navigate to the **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Deployment Settings**.

Step 2 Click the gear icon in the **Deployment Type**.
The **Configure your deployment** wizard opens.

Step 3 Select the deployment type as *Packaged CCE: 4000 Agents* or *Packaged CCE: 12000 Agents* from the drop-down list.

Step 4 Use the **Download Template** to get the CSV template for the selected deployment type.

Step 5 Fill the particulars in the file and save it.

Table 2: CSV Template Details

Column	Description	Required?	Permissible Values
name	Unique identifier for the machine	Yes	Name must start with an alphabet. Maximum length is limited to 128 characters. Valid characters are a-z, A-Z, 0-9, dot (.), underscore (_), or hyphen (-).

Column	Description	Required?	Permissible Values
machineType	MachineType Enum name	Yes	

Column	Description	Required?	Permissible Values
			Mandatory machines are: • CCE_ROGGER (applicable for 4000 Agents deployment) • CCE_ROUTER (applicable for 12000 Agents deployment) • CCE_LOGGER (applicable for 12000 Agents deployment) • CCE_AW • CUIC_PUBLISHER • CUIC_SUBSCRIBER • LIVE_DATA • IDS_PUBLISHER • IDS_SUBSCRIBER Optional machines: • CCE_PG • CVP • FINESSE_PRIMARY • FINESSE_SECONDARY • CM_PUBLISHER • CM_SUBSCRIBER • HDS • ECE (refers to ECE Data Server VM for ECE 400 agents and Services Server VM for ECE 1500 agents) • ECE_WEB_SERVER • CVP_REPORTING • GATEWAYS • CVVB • CUSP • SOCIAL_MINER • THIRD_PARTY_ MULTICHANNEL • MEDIA_SERVER

Column	Description	Required?	Permissible Values
			• **Note** • To enable addition of Media Servers in Packaged CCE 12.0(1), install the ICM12.0(1) ES and CVP ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html.
publicAddress	Public address	Yes	Valid IP address or hostname

Column	Description	Required?	Permissible Values

connectionInfo	Connection information of the machine	Required for CM_PUBLISHER, FINESSE_PRIMARY, ECE_WEB_SERVER, CVP, CVP_REPORTING, CUSP, GATEWAY and LIVE_DATA	Enter the username and password in the following format:
			`userName=<user>&password=<password>`
			For more information on the credentials of each component, see Table 1.
			ConnectionInfo is optional if you are configuring FTP for CVP (Media Server).
			Note To enable FTP configuration for CVP in Packaged CCE 12.0(1), install the ICM12.0(1) ES and CVP ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html.
			Append the FTP attributes to the username and password in the following format:
			`userName=<user>&password=<password>; ftpEnabled=<true or false> &ftpUserName=<ftp_username> &ftpPassword=<ftp_password> &ftpPort=<ftp_portnumber>`
			For more information on the FTP attributes, see FTP Section in the Add Media Server as External Machine.
			Note • Replace Ampersand (&) or equal sign (=) in usernames or passwords with their respective URL encoded values "%26" or "%3D".
			• Semicolon (;) delimits the Windows Administration credentials from FTP credentials.

privateAddress	Private address	Required for ROGGER, ROUTER, LOGGER, and PG	Valid IP address
peripheralSetName	Peripheral set name	Required for PG, CUCM, Finesse, CVP	Name can start with an alphabet. Maximum length is limited to 10 characters. Valid characters are a-z, A-Z, 0-9, dot (.), or an underscore (_).

Column	Description	Required?	Permissible Values
side	Side information	Yes	sideA sideB

Step 6 Upload the file and click **Next**.

Step 7 Wait for validation to be completed.

During the validation, tasks are performed depending on the components defined in the CSV template. For more information about the tasks, see Automated Initialization Tasks for 4000 and 12000 Agent Deployments, on page 73.

Note • If any of the performed tasks fails, then all the tasks are reverted.

If validation fails, then click **Back** to fix the issues in the file and upload the file again, else click **Done**.

The main site that is thus created is added to the Inventory page.

Automated Initialization Tasks for 4000 and 12000 Agent Deployments

Packaged CCE performs the following tasks during initialization.

Component	Automated Initialization Tasks	Other Dependent Components
Unified CCE PG	Creates the Agent Peripheral Gateway (PG) and PIMs	Cisco Unified Communications Manager (CUCM) and Cisco Finesse
	Creates the Media Routing PG (MR PG), without PIMs	None
	Creates the VRU PG and PIMs	Unified Customer Voice Portal
	Creates the routing client for each peripheral **Note** • Depending on your call flow requirements, create Network VRU labels in the Label list option using the *Configuration Manager* Tool. • Network VRU Type 10 and Type 2 must be created in the Network VRU Explorer using the Configuration Manager Tool. For more information, *see the online help in Configuration Manager Tool.*	None

Component	Automated Initialization Tasks	Other Dependent Components
Unified Customer Voice Portal	• Configures the Unified CVP Call Server components • Configures the Unified CVP VXML Server components • Configures the Unified CVP Media Server components	None
Unified CVP Reporting Server	Configures the Unified CVP Reporting Server components (not applicable for peripheral set)	None
Live Data	Redeploys Lives data	CUCM and Cisco Finesse

System Inventory for Packaged CCE 4000 Agents and 12000 Agents Deployment

You can access the Inventory after you have completed the change to a Packaged CCE deployment.

Access the Inventory by navigating to the **Unified CCE Administration** > **Infrastructure** > **Inventory**.

System Inventory contents are updated when you select or change the deployment type and after regular system scans. If a system scan detects VMs that do not conform to Packaged CCE requirements, the **Configure your deployment** pop-up window opens automatically, detailing the errors. You can access the Inventory again after you have corrected the errors and completed the **Configure your deployment** popup window.

For more details on **Server Status** rules, see the Monitor Server Status Rules for Packaged CCE 4000 and 12000 Agents Deployments, on page 77.

Note After a Packaged CCE deployment is initialized, you cannot switch to another deployment type.

Table 3: System Inventory Layout and Actions

Item	Notes	Actions
Set the Principal AW	Only one AW machine can be Principal AW at a time.	Specifying the Principal AW is required. The first SideA AW machine in the CSV file is the principal AW. The Principal AW (Admin Workstation) is responsible for managing background tasks that are run periodically to sync configuration with other solution components, such as SSO management, Smart Licensing, etc. The Principal AW is used by the following features: • File Transfer • Context Service Registration • SSO Registration and Enablement • Differential Sync You can change the Principal AW by selecting a different AW in the Inventory. Set the AW on which you make most of your configuration changes as the Principal AW. **To set the Principal AW:** **1.** Click the AW to open the Edit CCE AW window. **2.** Check the **PrincipalAW** check box. **3.** Unified CCE Diagnostic Framework Portico domain, username, and password. These credentials must be of a domain user who is a local administrator on all the CCE servers and valid on all Unified CCE components in your deployment (the Side A and Side B Unified CCE Roggers, PGs, and AW-HDS-DDSs). **Note** Every time the Active Directory credentials are updated, the credentials configured here must be updated as well. **4.** Click **Save**.

Item	Notes	Actions
View Statistics	Unified CVP and CVP Reporting Server	**Note** To enable CVP Statistics feature in Packaged CCE 12.0(1), install the ICM12.0(1) ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html. You can launch statistics by hovering over the following VMs and clicking the **Statistics** icon: • **Unified CVP** • **Unified CVP Reporting** For more information, see Unified CVP Statistics and Unified CVP Reporting Statistics.

Note If you change the password of any of the Packaged CCE components, you must update the password in the respective VM in the system inventory.

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).

Monitor Server Status Rules for Packaged CCE 4000 and 12000 Agents Deployments

In Packaged CCE 4000 and 12000 Agents deployments, the Inventory table displays an alerts icon for the Principal AW machine. Hover over the alert icon to view status of the machine.

Note If any machine in the Inventory is updated, it can take approximately three minutes for the status to appear.

Configure Cisco Unified Contact Center Enterprise PG

Note Repeat the following tasks each time you add the Peripheral Set to the Main Site or Remote Site. See Add and Maintain Peripheral Set for information on Peripheral Set.

Configuration Tasks
If the Peripheral Set contains CUCM PG: Install Cisco JTAPI Client on PG, on page 77 Install Cisco JTAPI Client on PG, on page 78 Set up CTI Server, on page 79
If the peripheral set contains VRU PG, manually restart the CVP Servers.
If the peripheral set contains MR PG, Add PIMs to the Media Routing Peripheral Gateway

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 78.

Before you begin

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

Procedure

Step 1 Open a browser window on the PG machine.

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

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

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

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

Download the JTAPI plugin file.

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

Step 7 Open the installer.

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

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

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

Step 11 Click **Finish**.

Step 12 Reboot the machine.

Install Cisco JTAPI Client on PG

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

Before you begin

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

Procedure

Step 1 Open a browser window on the PG machine.

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

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

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

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

Download the JTAPI plugin file.

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

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

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

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

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

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

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

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

```
Installation Complete.
```

Step 10 Reboot the machine.

What to do next

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

Set up CTI Server

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

Note Only users who are part of the local Administrators group can run Peripheral Gateway setup.

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.

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.

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.

Configure Cisco Unified Customer Voice Portal

The following table outlines the Cisco Unified Customer Voice Portal (CVP) configuration tasks for Packaged 4000 Agents deployment or 12000 Agents deployment.

Note The CVP configurations are site specific. Side A and Side B configurations per site must be the same.

Configuration Tasks
To secure communication between Call Server and ICM, see Secure GED 125 Communication between Call Server and ICM. For more information about securing CVP communication, see Unified CVP Security
For web secure communication, see pcce_b_admin-and-config-guide_120_appendix3.pdf#nameddest=unique_88
CVP Server Services Setup
Configure Media Server
Configure SNMP, on page 82

Configure SNMP

Use the Simple Network Management Protocol (SNMP) configuration to receive SNMP traps from the Cisco Customer Voice Portal (CVP) server. You can do this configuration in the CVP server using a configuration file.

Procedure

Step 1 Log in to the CVP server using Administrator credentials.

Step 2 Navigate to `C:\Cisco\CVP\conf\SNMPD.CNF`.

Step 3 Complete the following parameters to do the SNMP configuration:

Note Ensure to enter the parameter values in a single line, without a break.

Table 4: SNMP configuration parameters

Parameter	Description	Format

snmpCommunityEntry	Configure the SNMP agent that runs on the Unified CVP device to use the V1/V2 SNMP protocol to communicate with an SNMP management station; add and delete SNMP V1/V2c community strings and associate community strings with the device.	`snmpCommunityEntry <snmpCommunityIndex>`
		`<snmpCommunityName> <snmpCommunitySecurityName> <snmpCommunityContextEngineID> <snmpCommunityContextName> <snmpCommunityTransportTag> <snmpCommunityStorageType>`
		Example:
		`v2ccvp cvp cvp localSnmpID - - readOnly`

vacmSecurityToGroupEntry	Configure authentication group for V1/V2C SNMP protocol.	`vacmSecurityToGroupEntry <vacmSecurityModel> <vacmSecurityName> <vacmGroupName> <vacmSecurityToGroupStorageType>`
		Example:
		`vacmSecurityToGroupEntry snmpv2c cvp v2cNoAuthNoPrivGroup nonVolatile`

Parameter	Description	Format

snmpNotifyEntry	Configure the SNMP agent that runs on the Unified CVP device to use the V1/V2 SNMP protocol to communicate with an SNMP management station; configure a destination to receive SNMP notifications from an SNMP management station.	`snmpNotifyEntry <snmpNotifyName> <snmpNotifyTag> <snmpNotifyType> <snmpNotifyStorageType>`
		Example:
		`snmpNotifyEntry Descvp Descvp-TrapTag trap readOnly`

usmUserEntry	Configure the SNMP agent that runs on the Unified CVP device to use the V3 SNMP protocol to communicate with an SNMP management station; add and delete SNMP users and set their access privileges and associate SNMP users with devices.	`usmUserEntry <usmUserEngineID> <usmUserName> <usmUserAuthProtocol> <usmUserPrivProtocol> <usmUserStorageType> <usmTargetTag> <AuthKey> <PrivKey>`
		Example:
		`usmUserEntry localSnmpID cvp usmNoAuthProtocol usmNoPrivProtocol readOnly`

snmpNotifyEntry	Configure the SNMP agent that runs on the Unified CVP device to use the V3 SNMP protocol to communicate with an SNMP management station; configure a destination to receive SNMP notifications from an SNMP management station.	`snmpNotifyEntry <snmpNotifyName> <snmpNotifyTag> <snmpNotifyType> <snmpNotifyStorageType>`
		Example:
		`snmpNotifyEntry Descvp Descvp-TrapTag trap readOnly`

sysLocation	Configure the MIB2 System Group system location settings, and associate the MIB2 System Group with devices.	`<octetString>`
		Example:
		`MIBLoc`

sysContact	Configure the MIB2 System Group system contact and associate the MIB2 System Group with devices.	`<octetString>`
		For example:
		`MIBContact`

Parameter	Description	Format

snmpTargetAddrEntry	Configure SNMP trap receiver target IP.	`snmpTargetAddrEntry <snmpTargetAddrName>`
		`<snmpTargetAddrTDomain> <snmpTargetAddrTAddress> <snmpTargetAddrTimeout> <snmpTargetAddrRetryCount> <snmpTargetAddrTagList> <snmpTargetAddrParams> <snmpTargetAddrStorageType> <snmpTargetAddrTMask> <snmpTargetAddrMMS>`
		Example:
		`snmpTargetAddrEntry targetDesV2-Addr1 snmpUDPDomain 10.100.10.100:0 0 0 \ targetDesV2-TrapTag targetDesV2-TrapParams readOnly 255.255.255.255:0 2048`

snmpTargetParamsEntry	Configure the parameters to be used while sending notifications.	`snmpTargetParamsEntry <snmpTargetParamsName> <snmpTargetParamsMPModel> <snmpTargetParamsSecurityModel> <snmpTargetParamsSecurityName> <snmpTargetParamsSecurityLevel> <snmpTargetParamsStorageType>`
		Example:
		`snmpTargetParamsEntry params1 0 snmpv1 principal noAuthNoPriv nonVolatile`

Step 4 Save the changes.

Step 5 Go to `Services` and restart `Cisco CVP SNMP Management`.

License Management

Complete the following procedure to configure license in the CVP server (Call Server or Reporting Server).

Procedure

Step 1 Log in to the CVP server (Call Server or Reporting Server).

Step 2 Copy the license file into `C:\Cisco\CVP\conf\license` location.

Note The license file must be named as `cvp.license`.

Step 3 Restart the respective server.

Configure Cisco Unified Communications Manager

The following table outlines the Cisco Unified Communications Manager configuration tasks for Packaged CCE 4000 Agents deployment or 12000 Agents deployment.

.

Task
For details on CA and self-signed certificate, see Secure Communication on CUCM
Set Up Application User
Configure Fully Qualified Domain Name, on page 25
Configure Cisco Unified Communications Manager Groups, on page 25
Set Up Device Pool
Configure Conference Bridges, on page 26
Configure Media Termination Points, on page 26
Transcoder Configuration in Unified CM and IOS Gateway, on page 27
Configure Media Resource Groups, on page 27
Configure and Associate Media Resource Group List, on page 28
Configure CTI Route Point, on page 28
Configure Ingress Gateways for Locations-based Call Admission Control, on page 29
Add a SIP Profile in Unified CM, on page 29
Configure Trunk, on page 30
Configure Route Group, on page 30
Configure Route List, on page 31
Configure Route Pattern, on page 31
Configure A-Law Codec
Configure SNMP, on page 87
Configure Agent Desk Settings, on page 88

Set Up Device Pool

Complete the following procedure to configure a device pool.

Procedure

Step 1 Choose **System** > **device pool**.

Step 2 Click **Add new**.

Step 3 Provide an appropriate device pool name in **Device Pool Name**.

Step 4 Select a corresponding Call manager group in **Cisco Unified Communications Manager group**.

Step 5 Select appropriate **Date/Time Group** and **Region**.

Step 6 Select an appropriate Media resource group list in **Media Resource Group List.**

Step 7 Click **Save**.

Set Up Application User

Procedure

Step 1 In Unified Communications Manager, Choose **User Management** > **Application User**.

Step 2 In the Application User Configuration window, click **Add New**.

Step 3 Enter the User ID that is set in the Peripheral Gateway Setup.

Note The <site>_<peripheralsetname>_pguser is set on the PIM when the Peripheral Set is created.

Step 4 Enter a password of your choice.

Step 5 You must enter the same password set in the Peripheral Gateway Setup for CUCM PIM.

Step 6 Add the application user to the Standard CTI Enabled Group and Role:

a) Click **Add to Access Control Group**.
b) Select the **Standard CTI Enabled** group.
c) Select the **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** group.
d) Select the **Standard CTI Allow Control of Phones supporting Rollover Mode** group.
e) Click **Add Selected**.
f) Click **Save**.

Step 7 Associate the CTI route points and the phones with the application user.

Step 8 Click **Save**.

Configure A-Law Codec

Complete the following procedure to configure Unified Communications Manager.

Procedure

Step 1 Click the **System**.

Step 2 Select **Service Parameters**.

Step 3 Select a Server.

Step 4 Select the service as **Cisco Call Manager(Active)**.

Step 5 Under Clusterwide Parameters (system-location and region), ensure the following:

- **G.711 A-law Codec Enabled** is **Enabled**.
- **G7.11 mu-law Codec Enabled** to **Disabled**.

Step 6 Click **Save**.

Configure SNMP

Procedure

Step 1 Log in to the Cisco Unified Serviceability *(https://hostname of primary server:8443/ccmservice)* using administrator credentials.

Step 2 Select **SNMP** > **V1/V2c** > **Community String**.

Step 3 From **Server** drop-down list, select the server for which you want to configure a community string and click **Find**.

Step 4 Click **Add New** to add new community string.

a) Enter **Community String**.

Example:

public.

b) In **Host IP Addresses Information** field, choose **Accept SNMP Packets from any host**.

c) From **Access Privilages** drop-down list, select **ReadWriteNotify** option.

d) Check **Apply to All Nodes** check box to apply community string to all nodes in the cluster.

Information message will be displayed.

e) Click **OK**.

f) Click **Save**.

A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.

g) Click **OK**.

Step 5 Select **SNMP** > **V1/V2c** > **Notification Destination**.

Step 6 From **Server** drop-down list, select the server for which you want to configure a notification destination and click **Find**.

Step 7 Click **Add New** button to add new notification destination.

a) From **Host IP Addresses** drop-down list, select **Add New**.

b) In **Host IP Address** field, enter the Prime Collaboration server IP address .

c) In the **Port Number** field, enter the notification receiving port number.

Note Default port number is 162.

d) In **SNMP Version Information** field, select the SNMP Version V2C.

e) In **Notification Type Information** field; from **Notification Type** drop-down list, select **Trap**.

f) In **Community String Information** field; from **Community String** drop-down list, select Community String created in Step 4 from the drop-down list.

g) Check the **Apply to All Nodes** check box to apply community string to all nodes.

Information message will be displayed.

h) Click **OK**.

i) Click **Insert**.

A message is displayed, that indicates that changes will not take effect until you restart the SNMP primary agent. To continue the configuration without restarting the SNMP primary agent, click **Cancel**. To restart the SNMP primary agent service, click **OK**.

j) Click **OK**.

Configure Agent Desk Settings

Procedure

Step 1 From the AW server, open Configuration Manager, choose **Configure ICM** > **Enterprise** > **Agent Desk Settings** > **Agent Desk Settings List**. The Agent Desk Settings List dialog box opens.

Step 2 Click **Retrieve** and then Click **Add**.

Step 3 Fill in the Attributes tab information:

Name. Enter a name for the agent desk settings that is unique within the enterprise.

Ring No Answer Time. Enter the number of seconds (between 1 and 120) that a call may ring at the agent's station. If you are deploying the Unified CVP, make sure this number is less than the number set for the No Answer Timeout for Router Requery that you set in the Unified CVP.

If you configure this timer, you do not need to configure the Unified Communications Manager Call Forward on No Answer for agent extensions in the Unified Communications Manager, unless you want them to be used when the agent is not logged in. If you set the Unified Communications Manager Call Forward No Answer time, enter a value at least 3 seconds higher than the Ring No Answer Time on each Unified Communications Manager node.

Ring no answer dialed number. Enter the Unified CCE DN associated with the routing script that you want to use to reroute a call that an agent has not answered. If you are deploying the Unified CVP, leave this field blank.

Logout non-activity Time. Enter the number of seconds (between 10 and 7200) in which the agent can remain in Not Ready state before Unified CCE automatically logs out the agent.

Work Mode on Incoming. Select whether wrap-up is required following an incoming call. Select an option from the drop-down list.

Work Mode on Outgoing. Select whether wrap-up is required following an outgoing call. Select an option from the drop-down list.

Wrap Up Time. Enter the amount of time, in seconds, allocated to an agent to wrap up a call.

Assist Call Method. Select whether Unified CCE creates a consultative call or a blind conference call for a supervisor assistance request.

Emergency Alert Method. Select whether the Unified CCE creates a consultative call or a blind conference call for an emergency call request.

Blind conference is not supported if the call may queue on a VRU.

Description. Enter additional optional information about the agent desk settings.

Step 4 Use the following boxes to select or de-select miscellaneous settings:

Auto-answer. Indicates whether calls to the agent are automatically answered. The agent is not required to take any action to answer the call. If a second call comes in while a call is in progress, the call is not automatically answered. This is the same behavior as with Unified Communications Manager.

If you enable auto-answer, you must also configure the agent phone in Unified Communications Manager to turn the speakerphone or headset (or both) to ON. If you turn *only* the headset to ON, the agent must also turn the phone headset button to ON.

In a multi-line enabled environment with auto-answer selected, if you are on a call on your non-ACD line, the call will *not* auto-answer. However, if you turn on Unified Communications Manager Auto Answer, the call *will* answer.

Idle Reason Required. Indicates whether an agent is required to enter a reason before entering the Idle state.

Logout Reason Required. Indicates whether an agent is required to enter a reason before logging out.

Auto Record on Emergency. Indicates in a record request is automatically sent when an emergency call request starts.

Cisco Unified Mobile Agent (check box). Enables the Unified Mobile Agent feature so that the agent can log in remotely and take calls from any phone. For more information about the Unified Mobile Agent, see the *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.html.

Step 5 Click **Save** and then click **Close**.

Note For any change, you perform in the **Agent Desk Settings** to take effect, log out and then log in to the Finesse Agent Desktop.

Configure Cisco Unified Intelligence Center

Follow this sequence to configure the Cisco Unified Intelligence Center for Packaged CCE 4000 and 12000 Agents deployment

Sequence	Task
1	For details on security certificate, see *Cisco Unified Intelligence Center User Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html
3	Configure Unified Intelligence Center Data Sources for External HDS, on page 32
3	Download Report Bundles, on page 33
4	Import Reports, on page 33

Sequence	Task
5	Configure Unified Intelligence Center Administration, on page 35

Configure Cisco Finesse

Follow this sequence to configure the Cisco Finesse for Packaged CCE 4000 Agents deployment or 12000 Agents deployment

Sequence	Task
1	For details on CA certificate, refer the *Cisco Finesse Administration Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html
2	For details on self-signed certificate, see Add Finesse Certificate to AW Machine
3	Navigate to **Infrastructure Settings** > **Device Configuration** > **Finesse** to configure, and then select the **Site** and **Peripheral Set** of the Finesse server. Configure Contact Center Enterprise Administration and Data Server Settings Configure Contact Center Enterprise CTI Server Settings
4	Configure Contact Center Agents and Routing for Live Data Reports, on page 36
5	Restart the Cisco Tomcat Service, on page 90
6	Live Data Reports, on page 36
7	Configure SNMP, on page 87

Restart the Cisco Tomcat Service

After you change and save any value on Unified CCE Administration server settings, you must restart the Cisco Tomcat Service on the primary Cisco Finesse server.

Procedure

Step 1 Enter **utils service stop Cisco Tomcat** command, to stop the Cisco Tomcat service.

Step 2 Enter **utils service start Cisco Tomcat** command, to start the Cisco Tomcat service.

Configure Cisco Finesse Administration

- Obtain and Upload a CA Certificate, on page 91
- Accept Security Certificates, on page 94

Obtain and Upload a CA Certificate

Note This procedure applies only if you are using HTTPS.

This procedure is optional. If you are using HTTPS, you can choose to obtain and upload a CA certificate or you can choose to use the self-signed certificate provided with Cisco Finesse.

To open Cisco Unified Operating System Administration, enter the following URL in your browser: `https://FQDN of primary Finesse server:8443/cmplatform`.

Sign in using the username and password for the application user account created during Cisco Finesse installation.

Procedure

Step 1 Generate a CSR as follows.

a) Select **Security > Certificate Management > Generate CSR**.
b) From the certificate name drop-down list, select **tomcat**.
c) Click **Generate CSR**.

Step 2 Download the CSR.

a) Select **Security > Certificate Management > Download CSR**.
b) From the certificate name drop-down list, select **tomcat**.
c) Click **Download CSR**.

Step 3 Use the CSR to obtain the signed application certificate and the CA root certificate from the Certificate Authority.

Step 4 When you receive the certificates, select **Security > Certificate Management > Upload Certificate**.

Step 5 Upload the root certificate.

a) Choose **tomcat-trust** from **Certificate Name** drop-down list.
b) Click **Browse** and open the root certificate file, in **Upload File** field.
c) Click **Upload File**.

Step 6 Upload the application certificate.

a) Choose **tomcat** from **Certificate Name** drop-down list.
b) Enter the name of the CA root certificate in the **Root Certificate** field.
c) Click **Browse** and open the root certificate file, in **Upload File** field.
d) Click **Upload File**.

Step 7 After the upload is complete, sign out from Cisco Finesse.

Step 8 Access the CLI on the primary Cisco Finesse server.

Step 9 Enter **utils service restart Cisco Finesse Notification Service** command to restart the Cisco Finesse Notification service.

Step 10 Enter **utils service restart Cisco Tomcat** command to restart the Cisco Tomcat service.

Step 11 Upload the root certificate and application certificate to the secondary Cisco Finesse server.

Note Enter the following URL in browser: `https://FQDN of secondary Finesse server:8433/cmplatform`, to open **Cisco Unified Operating System Administration** for the secondary server.

Step 12 Access the CLI on the secondary Cisco Finesse server and restart the Cisco Finesse Notification Service and the Cisco Tomcat Service.

Deploy Certificate in Browsers

Download CA certificate

This procedure assumes that you are using the Windows Certificate Services. Perform the following steps to retrieve the root CA certificate from the certificate authority. After you retrieve the root certificate, each user must install it in the browser used to access Finesse.

Procedure

Step 1 On the Windows domain controller, run the CLI command certutil -ca.cert *ca_name*.cer, in which *ca_name* is the name of your certificate.

Step 2 Save the file. Note where you saved the file so you can retrieve it later.

Set Up CA Certificate for Internet Explorer Browser

After obtaining and uploading the CA certificates, either the certificate must be automatically installed via group policy or all users must accept the certificate.

In environments where users do not log directly in to a domain or group policies are not utilized, every Internet Explorer user in the system must perform the following steps once to accept the certificate.

Procedure

Step 1 In Windows Explorer, double-click the *ca_name*.cer file (in which *ca_name* is the name of your certificate) and then click **Open**.

Step 2 Click **Install Certificate** > **Next** > **Place all certificates in the following store**.

Step 3 Click **Browse** and select **Trusted Root Certification Authorities**.

Step 4 Click **OK**.

Step 5 Click **Next**.

Step 6 Click **Finish**.

A message appears that states you are about to install a certificate from a certification authority (CA).

Step 7 Click **Yes**.

A message appears that states the import was successful.

Step 8 To verify the certificate was installed, open Internet Explorer. From the browser menu, select **Tools** > **Internet Options**.

Step 9 Click the **Content** tab.

Step 10 Click **Certificates**.

Step 11 Click the **Trusted Root Certification Authorities** tab.

Step 12 Ensure that the new certificate appears in the list.

Step 13 Restart the browser for certificate installation to take effect.

Note If using Internet Explorer 11, you may receive a prompt to accept the certificate even if signed by private CA.

Set Up CA Certificate for Firefox Browser

Every Firefox user in the system must perform the following steps once to accept the certificate.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 From the Firefox browser menu, select **Options**.

Step 2 Click **Advanced**.

Step 3 Click the **Certificates** tab.

Step 4 Click **View Certificates**.

Step 5 Click **Authorities**.

Step 6 Click **Import** and browse to the *ca_name*.cer file (in which *ca_name* is the name of your certificate).

Step 7 Check the **Validate Identical Certificates** check box.

Step 8 Restart the browser for certificate installation to take effect.

Deploy Root Certificate for Browsers

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's browser. Adding the certificate automatically simplifies user requirements for configuration.

Note To avoid certificate warnings, each user must use the fully-qualified domain name (FQDN) of the Finesse server to access the desktop.

Procedure

Step 1 On the Windows domain controller, navigate to **Administrative Tools** > **Group Policy Management**.

Note Users who have strict Group Policy defined on the Finesse Agent Desktop are required to disable **Cross Document Messaging** from **Group Policy Management** to ensure proper functioning of Finesse on browser.

Step 2 Right-click Default Domain Policy and select **Edit**.

Step 3 In the Group Policy Management Console, go to **Computer Configuration** > **Policies** > **Window Settings** > **Security Settings** > **Public Key Policies**.

Step 4 Right-click Trusted Root Certification Authorities and select **Import**.

Step 5 Import the *ca_name*.cer file.

Step 6 Go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Certificate Services Client - Auto-Enrollment**.

Step 7 From the Configuration Model list, select **Enabled**.

Step 8 Sign in as a user on a computer that is part of the domain and open browser.

Step 9 If the user does not have the certificate, run the command **gpupdate.exe /target:computer /force** on the user's computer.

Set Up CA Certificate for Chrome and Edge Chromium (Microsoft Edge) Browsers

Procedure

Step 1 In the browser, go to **Settings**.

Step 2 In the Chrome browser, select **Advanced Settings** > **Privacy and Security**, click **Manage Certificates**.

Step 3 In the Microsoft Edge browser, select **Privacy, search, and services**. Under **Security**, click **Manage Certificates**.

Step 4 Click **Trusted Root Certification Authorities** tab.

Step 5 Click **Import** and browse to the *ca_name*.cer file.
In the **Trusted Root Certification Authorities** tab, ensure that the new certificate appears in the list.

Step 6 Restart the browser for the certificate to install.

Accept Security Certificates

Ensure that the pop-ups are enabled for the Finesse desktop.

After you enter the Finesse desktop URL in your browser, the procedure to add a certificate is as follows:

Install certificates on Windows operating system:

The procedure to add a certificate varies for each browser. The procedure for each browser is as follows:

Internet Explorer

Note

If you are using a Windows client, signed in as a Windows user, you must run Internet Explorer as an administrator to install the security certificates. In your Start menu, right-click Internet Explorer and select Run as administrator.

Contact your administrator if you do not have the required permissions to install the security certificates.

1. A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)** link to open the Finesse sign in page. The Finesse sign in screen appears with a certificate error in the address bar.
2. Click on the certificate error that appears in the address bar and then click **View Certificates**.
3. In the **Certificate** dialog box, click **Install Certificate** to open the **Certificate Import Wizard**.
4. Select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users.
5. On the **Certificate Import Wizard**, click **Next**.
6. Select **Place all certificates in the following store** and click **Browse**.
7. Select **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears.
9. Click **Yes** to install the certificate. The **Certificate Import** dialog box appears.
10. Click **OK** and close the **Certificate Import** dialog box.
11. Close the browser tab. The accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Note

To remove the certificate error from the desktop, you must close and reopen your browser.

Firefox

1. On **Your connection is not secure** page, click **Advanced** > **Add Exception**.

   Note

   Ensure that the **Permanently store this exception** box is checked.

2. Click **Confirm Security Exception**.
3. On and click **Sign In**.
4. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.

5. On the browser tab, click **I Understand the Risks** > **Add Exception**. Ensure that the **Permanently store this exception** box is checked.
6. Click **Confirm Security Exception**. The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Repeat the preceding steps for all the certificate links. After you accept all the certificates, the sign-in process is complete.

Chrome and Edge Chromium (Microsoft Edge)

1. A page appears that states your connection is not private. To open the Finesse sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.
2. Enter your agent ID or username, password, and extension, and then click **Sign In**.
3. In the **SSL Certificate Not Accepted** dialog box, click the certificate link. A browser tab opens for the certificate that you must accept.
4. On the browser tab,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

   The browser tab closes after you accept the certificate and the accepted certificate link is removed from the **SSL Certificate Not Accepted** dialog box. Close the browser tab if it does not automatically close.

Note If you click the certificate link and do not accept it, the certificate link stays enabled in the **SSL Certificate Not Accepted** dialog box. The certificate error appears every time you sign in. The procedure to permanently accept the certificate is as follows.

5. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (not valid)**.

   The **Certificate** dialog box appears.
6. In the **Details** tab, click **Copy to File**. The **Certificate Export Wizard** appears.
7. Click **Next**.
8. Keep the default selection **DER encoded binary X.509 (.CER)** and click **Next**.
9. Click **Browse** and select the folder in which you want to save the certificate, enter a recognizable file name and click **Save**.
10. Browse to the folder where you have saved the certificate (**.cer** file), right-click on the file, and click **Install Certificate**. The **Certificate Import Wizard** appears.
11. Keep the default selection **Current User** and click **Next**.

12. Select **Place all certificates in the following store** and click **Browse**. The **Select Certificate Store** dialog box appears.
13. Select **Trusted Root Certification Authorities** and click **OK**.
14. Click **Next** and then click **Finish**. A **Security Warning** dialog box appears that asks if you want to install the certificate.
15. Click **Yes**. A **Certificate Import** dialog box that states the import was successful appears.

Close the browser and sign in to Finesse. The security error does not appear in the address bar.

Install certificates on macOS:

The procedure to download a certificate varies for each browser. The procedure for each browser is as follows:

Chrome and Edge Chromium (Microsoft Edge)

1. A warning page appears which states that your connection is not private. To open the Finesse Console sign in page,

   In Chrome, click **Advanced** > **Proceed to <Hostname> (unsafe)**.

   In Microsoft Edge, click **Advanced** > **Continue to <Hostname> (unsafe)**.

2. Click on the certificate error that appears in the address bar and then,

   In Chrome, select **Certificate (Invalid)**.

   In Microsoft Edge, select **Certificate (Not Valid)**.

   A certificate dialog box appears with the certificate details.

3. Drag the **Certificate** icon to the desktop.
4. Double-click the certificate. The **Keychain Access** application opens.
5. In the right pane of Keychains dialog, browse to the certificate, right-click on the certificate, and select **Get Info** from the options that are listed. A dialog appears with more information about the certificate.
6. Expand **Trust**. From the **When using this certificate** drop-down, select **Always Trust**.
7. Close the dialog box that has more information about the certificate. A confirmation dialog box appears.
8. Authenticate the modification of Keychains by providing a password.
9. The certificate is now trusted, and the certificate error does not appear on the address bar.

Firefox

1. In your Firefox browser, enter the Finesse desktop URL. A warning page appears which states that there is a security risk.
2. Click **Advanced** and then click **View Certificate** link. The **Certificate Viewer** dialog box appears.
3. Click **Details** and then click **Export**. Save the certificate (**.crt** file) in a local folder.

Note If **.crt** file option is not available, select **.der** option to save the certificate.

4. From the menu, select **Firefox** > **Preferences**. The **Preferences** page is displayed.
5. In the left pane, select **Privacy & Security**.
6. Scroll to the **Certificates** section and click **View Certificates ...**. The **Certificate Manager** window is displayed.
7. Click **Import** and select the certificate.
8. The certificate is now authorized, and the certificate error does not appear on the address bar.

Configure Live Data

Sequence	Task
1	Initial Setup for Live Data, on page 98
2	Configure Live Data with AW, on page 98
3	Configure Live Data Machine Services, on page 99
4	Configure Live Data for Unified Intelligence Center Data Sources, on page 100
6	Restart Live Data, on page 101

Initial Setup for Live Data

For Live Data to work on Packaged CCE 4000 and 12000 Agents deployment, do the following on both Side A and Side B Logger:

Procedure

Step 1 Launch **Microsoft SQL Server Management Studio** and select the Logger database (Side A or Side B appropriately).

Step 2 Run the queries in the file `C:\icm\install\LiveDataMachineServiceCorrection.sql`.

Note From AW Machine, run the Initialize Local Database tool.

Configure Live Data with AW

Configure Live Data with AW to access the primary AW DB and the secondary AW DB. The command also automatically tests the connection from Live Data to the primary or secondary AW, checks to see if you (as the configured user) have appropriate AW DB access, and reports the results.

You can use the optional skip-test parameter if you do not want to perform the test. When you include the skip-test parameter, the command does not check if you (as the configured user) have appropriate AW DB access and does not report results.

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

Before you begin

Before you can configure Live Data, you must first configure a SQL user (with special permissions) to work with Live Data.

The SQL administrative user "sa" or a user with sysadmin privileges must then run the following SQL queries on the primary system database for the SQL user who is configured to work with Live Data:

```
USE master
GO
GRANT CONTROL ON CERTIFICATE :: UCCESymmetricKeyCertificate TO "<user>"
GRANT VIEW DEFINITION ON SYMMETRIC KEY :: UCCESymmetricKey TO "<user>"
```

Procedure

Step 1 Log in to your Live Data server.

Step 2 Run the following command to configure Live Data with the primary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results.

The skip-test parameter is optional. Include it only if you do not want to perform the test.

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

Step 3 Run the following command to configure Live Data with the secondary AW DB. The command automatically tests the connection from Live Data, checks the user permission, and displays results.

The skip-test parameter is optional. Include it only if you do not want to perform the test.

set live-data aw-access secondary *addr* *port* *db* *user* [*skip-test*]
You can also optionally run the following command at any time to show and test the AW configuration that you set from Live Data to the primary and secondary AW DBs.

The skip-test parameter is optional. Include it only if you do not want to perform the test.

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

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 100.

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.
- Cisco Unified Communications Manager (CUCM) PG, generic PGs with CUCM peripherals, Unified CCE Gateway PGs, and Avaya 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*

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, 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, see Certificates for Live Data.

Configure Cisco Identity Service

The following table outlines the Cisco Identity Service configuration task for Packaged 2000 Agent deployments to 12000 Agent deployments.

.

Sequence	Task
1	Add IdS Certificate to AW Machine
2	Configure an Identity Provider (IdP), on page 102
3	Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256, on page 102
4	Configure the Cisco Identity Service, on page 108
5	Set Up the External HDS for Single Sign-On

Sequence	Task
6	Register Components and Set Single Sign-On Mode, on page 110 For more information about configuring the Single Sign-On feature, see *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.
7	Cisco SNMP Setup, on page 21 (optional)

Configure an Identity Provider (IdP)

To support SSO for the contact center solution, configure an Identity Provider (IdP) that is compliant with the Security Assertion Markup Language 2.0 (SAML v2) Oasis standard. The IdP stores user profiles and provides authentication services to the contact center solution.

Note For a current list of supported Identity Provider products and versions, see the *Contact Center Enterprise Compatibility Matrix*.

This section provides sample configuration information for Microsoft AD FS.

Follow this sequence of tasks to configure the Identity Provider.

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 103
2	Set Authentication Type. See Authentication Types, on page 103.
3	Configure an Identity Provider (IdP), on page 102
4	Enable Signed SAML Assertions, on page 106
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 107

Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256

This procedure is useful for upgrades from version 11.x where the only Secure Hash Algorithm supported was SHA-1.

.

Perform this procedure after the upgrade has completed successfully.

Procedure

Step 1 From browser in AD FS Server, login to Cisco IdS admin interface `https://<Cisco IdS server address>:8553/idsadmin`.

Step 2 Click **Settings**.

Step 3 Click **Security** tab.

Step 4 Click **Keys and Certificates**.

Note After this step, Single Sign On will stop working until you complete Step 8.

Step 5 Regenerate SAML Certificate with SHA-256 Secure Hash Algorithm. In the SAML Certificate section, change Secure Hash algorithm dropdown menu to SHA-256 and then click **Regenerate** button

Step 6 Download new metadata file. Click on **IdS Trust** tab and then click download button.

Step 7 Change Secure Hash Algorithm in AD FS Relaying Party Trust configuration. In AD FS server, open AD FS Management. Go to **ADFS** ->**Trust Relationships**->**Relying Party Trusts**, right click on existing Relying Party Trust for Cisco IdS and then click on Properties. In the Advanced Tab, change the Secure Hash Algorithm to **SHA-256.** Click **Apply**.

Step 8 Update Relying party trust on AD FS. From AD FS Server, run the following Powershell command:

```
Update-AdfsRelyingPartyTrust -MetadataFile <path to Step 6 new MetaData File> -TargetName
        <Relying Party Trust Display Name>
```

Install and Configure Active Directory Federation Services

Follow Microsoft instructions and guidelines to install Microsoft Active Directory Federation Services (AD FS).

For example, see *Active Directory Federation Services Overview* at https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspx

- For AD FS 2.0, see *AD FS Content Map* at http://aka.ms/adfscontentmap.

Note Cisco IdS does not support AD FS Automatic Certificate Rollover. If the AD FS certificate gets rolled over, then re-establish the trust relationship between the IdS and AD FS.

Note The Secure Hash Algorithm (SHA) used for signature verification between:

- IdP and Cisco IdS: SHA-1, SHA-256
- Cisco IdS and the application browsers: SHA-256

Authentication Types

Cisco Identity Service supports form-based authentication of the Identity Provider.

For information on enabling form-based authentication in ADFS, see Microsoft documentation:

- For ADFS 2.0 see https://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx
- For ADFS 3.0 see https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

For Kerberos authentication to work, ensure to disable the form-based authentication and follow the steps provided in *Kerberos Authentication (Integrated Windows Authentication)*.

- In AD FS on Windows Server , set the Authentication Type to Forms-based authentication (FBA). Refer to the following Microsoft TechNet article, http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx
- In AD FS on Windows Server, set the Authentication Policy to Forms Authentication. Refer to the following Microsoft TechNet article, https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/

Integrate Cisco IdS to the Shared Management AD FS

Procedure

Step 1 In AD FS, be sure that the default Authentication Type is set to Forms. (Cisco Identity Service requires the Identity Provider to provide form-based authentication.) See the Microsoft AD FS documentation for details.

Step 2 In AD FS server, open **AD FS Management**.

Step 3 Right-click **AD FS** -> **Trust Relationships** -> **Relying Party Trust**.

Step 4 From the menu, choose **Add Relying Party Trust** to launch the **Add Relying Party Trust Wizard**.

Step 5 In the **Select Data Source** step, choose the option **Import data about the relying party from a file**.

Step 6 **Browse** to the `sp.xml` file that you downloaded from Cisco Identity Server and complete the import to establish the relying party trust.

Step 7 Select the step **Specify Display Name**, and add a significant name you can use to identify the Relying Party Trust.

Step 8 For AD FS in Windows Server, select the option **I do not want to configure multi-factor authentication settings for the relying party at this time** in the Step **Configure Multi-factor Authentication Now**.

This step does not appear in AD FS 2.0 or 2.1. Continue with the next step.

Step 9 In the Step Choose Issuance Authorization Rules, select the option **Permit all users to access this relying party** and click **Next**.

Step 10 Click **Next** again to finish adding the relying party.

Step 11 Right-click on the **Relying Party Trust** and click **Properties**. Select the **Identifiers** tab.

Step 12 On the Identifiers tab, Set **Display name** to the name you specified when creating the Relying Party Trust, and set the **Relying party identifier** to the **fully qualified hostname** of the Cisco Identity Server from which `sp.xml` was downloaded.

Step 13 Still in **Properties**, select the **Advanced** tab.

Step 14 Select **secure hash algorithm** as **SHA-1** and then click **OK**.

Note In the following steps, you configure two claim rules to specify the claims that are sent from AD FS to Cisco Identity Service as part of a successful SAML assertion:

- A claim rule with the following custom claims, as AttributeStatements, in the assertion:
  - **uid** - Identifies the authenticated user in the claim sent to the applications.
  - **user_principal** - Identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.
- A second claim rule that is a NameID custom claim rule specifying the fully qualified domain name of the AD FS server and the Cisco IdS server.

Follow the steps to configure these rules.

Step 15 In **Relying Party Trusts**, right-click on the Relying Party Trust you created, and click **Edit Claim Rules**.

Step 16 Follow these steps to add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

a) In the **Issuance Transform Rules** tab, click **Add Rule**.
b) In the Step **Choose Rule Type**, select the claim rule template **Send LDAP Attributes as Claims** and click **Next**.
c) In the **Configure Claim Rule** step, in the **Claim rule name** field, enter **NameID**.
d) Set the **Attribute store** drop-down to **Active Directory**.
e) Set the table **Mapping of LDAP attributes to outgoing claim types** to the appropriate **LDAP Attributes** and the corresponding **Outgoing Claim Type** for the type of user identifier you are using:

   - When the identifier is stored as a **SAM-Account-Name** attribute:
     1. Select an **LDAP Attribute**of **SAM-Account-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
     2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).
   - When the identifier is a UPN:
     1. Select an **LDAP Attribute**of **User-Principal-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
     2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).

   Note The SAM-Account-Name or UPN choice is based on the User ID configured in the AW.

Step 17 Follow these steps to add a second rule with the template **custom claim rule**.

a) Select **Add Rule** on the **Edit Claim Rules** window.
b) Select **Send Claims Using Custom Rule**.
c) Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.
d) Add the following rule text:

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"]
 =>
 issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
 Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
 Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
 "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"]
 =
 "http://<AD FS Server FQDN>/adfs/services/trust",

Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
 =
 "<fully qualified domain name of Cisco IdS>");
```

e) Edit the script as follows:

- Replace **<ADFS Server FQDN>** to match exactly (including case) the ADFS server FQDN (fully qualified domain name.)
- Replace **<Cisco IdS server FQDN>** to match exactly (including case) the Cisco Identity Server FQDN.

Step 18 Click **OK**.

Enable Signed SAML Assertions

Enable Signed SAML Assertions for the Relying Party Trust (Cisco Identity Service).

Procedure

Step 1 Click **Start** and type **powershell** in the Search field to display the Windows Powershell icon.

Step 2 Right-click on the Windows Powershell program icon and select **Run as administrator**

Note All PowerShell commands in this procedure must be run in Administrator mode.

Step 3 Run the command, **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"**.

Note Set <Relying Party Trust Display Name> to exactly match (including case) the Identifier tab of the Relying Party Trust properties.

For example:

```
Set-ADFSRelyingPartyTrust -TargetName CUICPub.PCCERCDN.cisco.com
-SamlResponseSignature "MessageAndAssertion".
```

Step 4 Navigate back to the Cisco Identity Service Management window.

Step 5 Click **Settings**.
By default **IdS Trust** tab is displayed.

Step 6 On the Download SAML SP Metadata and Upload IdP Metadata windows, click Next as you have already established trust relationship between IdP and IdS.

Step 7 On the AD FS authentication window, provide the login credentials.

Step 8 On successful SSO setup, the message "SSO Configuration is tested successfully" is displayed.

Note If you receive the error message "An error occurred", ensure that the claim you created on the AD FS is enabled.

If you receive the error message "IdP configuration error: SAML processing failed", ensure that the rule has the correct names for Ids and AD FS.

Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID

By default, the sign-in page presented to SSO users by AD FS in Windows Server requires a username that is a UPN. Usually this is an email format, for example, user@cisco.com. If your contact center solution is in a single domain, you can modify the sign-in page to allow your users to provide a simple User ID that does not include a domain name as part of the user name.

There are several methods you can use to customize the AD FS sign-in page. Look in the Microsoft AD FS in Windows Server documentation for details and procedures to configure alternate login IDs and customize the AD FS sign-in pages.

The following procedure is an example of one solution.

Procedure

Step 1 In the AD FS **Relying Party Trust**, change the NameID claim rule to map the chosen LDAP attribute to **uid**.

Step 2 Click the Windows **Start** control and type **powershell** in the Search field to display the Windows Powershell icon.

Step 3 Right-click on the Windows Powershell program icon and select **Run as administrator**

All PowerShell commands in this procedure must be run in Administrator mode.

Step 4 To allow sign-ins to AD FS using the sAMAccountName, run the following Powershell command:

```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID sAMAccountName
-LookupForests myDomain.com
```

In the LookupForests parameter, replace `myDomain.com` with the forest DNS that your users belong to.

Step 5 Run the following commands to export a theme:

```
mkdir C:\themeExport-AdfsWebTheme –Name default –DirectoryPath c:\theme
```

Step 6 Edit `onload.js` in `C:\theme\script` and add the following code at the bottom of the file. This code changes the theme so that the AD FS sign-in page does not require a domain name or an ampersand, "@", in the username.

```
// Update the placeholder text to not include the domain
var userNameInput = document.getElementById("userNameInput");
if (userNameInput) {
 userNameInput.setAttribute("placeholder", "Username");
}

// Override submitLoginRequest to not have the "@" check
Login.submitLoginRequest = function () {
 var u = new InputUtil();
 var e = new LoginErrors();
 var userName = document.getElementById(Login.userNameInput);
 var password = document.getElementById(Login.passwordInput);
 if (!userName.value) {
  u.setError(userName, e.userNameFormatError);
  return false;
 }
 if (!password.value) {
  u.setError(password, e.passwordEmpty);
  return false;
 }
 document.forms['loginForm'].submit();
 return false;
};
```

Step 7 In Windows PowerShell, run the following commands to update the theme and make it active:

```
Set-AdfsWebTheme -TargetName custom -AdditionalFileResource
@{Uri=’/adfs/portal/script/onload.js’;path="c:\theme\script\onload.js"}

Set-AdfsWebConfig -ActiveThemeName custom
```

Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings that are related to security, identify clients of the Cisco IdS service, and set log levels. If desired, enable Syslog format.

Note In Packaged CCE 4000 or 12000 Agent deployments:

- Unified CCE AW, Unified Intelligence Center, Finesse, and external HDS gets automatically associated with a default Cisco Identity Service (Cisco IdS).
- Make sure that the Principal AW is configured, and is functional before using the Single Sign-On tool in the Unified CCE Administration. Also, add the SSO-capable machines to the Inventory.

In Packaged CCE 2000 Agent deployments, you must manually associate an external HDS with a default Cisco Identity Service (Cisco IdS). For more information, see Set Up the External HDS for Single Sign-On.

Procedure

Step 1 In the Unified CCE Administration, choose **Overview** > **Infrastructure Settings** > **Device Configuration** > **Single Sign-On Setup**.

Note Use a log in name in the format *username@FQDN* to log in to the Unified CCE Administration.

The **Identity Service Nodes**, **Identity Service Settings**, and **Identity Service Clients** tabs appear.

Step 2 Click **Identity Service Nodes**.

You can view the overall Node level and identify which nodes are in service. You can also view the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

Step 3 Click **Identity Service Settings**.

Step 4 Click **Security**.

Step 5 Click **Tokens**.
Enter the duration for the following settings:

- **Refresh Token Expiry** -- Refresh token is used to get new Access tokens. This parameter specifies the duration after which the Refresh token expires. The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- Authorization code is used to get Access tokens from Cisco IdS. This parameter specifies the duration after which the Authorization code expires. The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- Access token contains security credentials used to authorize clients for accessing resource server. This parameter specifies the duration after which the Access token expires. The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 6 Set the **Encrypt Token** (optional); the default setting is **On**. Use this configuration to secure the tokens as Cisco IdS issues tokens in both plain text or encrypted formats.

Step 7 Click **Save**.

Step 8 Click **Keys and Certificates**.
The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration. An Administrator regenerates the Encryption/Signature key when it is exposed or compromised.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful. SAML certificate is regenerated when it expires or when IdS relying party trust configuration on IdP is deleted.

Note Establish the trust relationship again whenever the Encryption keys or SAML certificates are regenerated.

Step 9 Click **Save**.

Step 10 Click **Identity Service Clients**.
On the **Identity Service Clients** tab, you can view the existing Cisco IdS clients, with the client name, client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the name of client.

Step 11 To add a client on the **Identity Service Clients** tab:

a) Click **New**.
b) Enter the name of client.
c) Enter the Redirect URL. To add more than one URL, click the plus icon.
d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

Step 12 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

Step 13 Click **Identity Service Settings**.

Step 14 Click **Troubleshooting** to perform some optional troubleshooting.

Step 15 From the **Log Level** drop-down list, set the local log level by choosing **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 16 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host** (Optional) field.

Step 17 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Register Components and Set Single Sign-On Mode

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically.

Before you begin

- Configure the Cisco Identity Service (Cisco IdS).
- Disable popup blockers. It enables viewing all test results correctly.
- If you are using Internet Explorer, verify that:
  - It is not in the Compatibility Mode.
  - You are using the fully qualified domain name of AW to access the CCE Administration (for example, **https://<FQDN>/cceadmin**).

Procedure

Step 1 In the Unified CCE Administration, navigate to **Features** > **Single Sign-OnOverview** > **Infrastructure Settings** > **Device Configuration** > **Single Sign-On Setup**.

Step 2 Click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error and click **Retry**.

Step 3 Click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when presented with a log in dialog, log in as a user with SSO credentials.

The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click **Test** again.

Test results are not saved. If you refresh the page, run the test again before enabling SSO.

Step 4 Select the SSO mode for the system from the **Set Mode** drop-down menu:

- Non-SSO: This mode disables SSO for all agents and supervisors. Users log in using existing Active Directory-based local authentication.
- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.

Packaged CCE 12000 Agents Deployment

Follow this sequence to configure components for Packaged CCE 12000 Agents deployment.

Sequence	Task
1	Configure CCE Component, on page 112
2	Configure Cisco Unified Customer Voice Portal, on page 81
3	If Media Server is external, Configure Media Server
4	Configure Cisco Unified Communications Manager, on page 85
5	Configure Cisco Unified Intelligence Center, on page 89
6	Configure Cisco Finesse, on page 90
7	Configure Live Data, on page 98
8	Configure Cisco Identity Service, on page 101
9	Configure Cisco Unified Customer Voice Portal Reporting Server, on page 39 (optional)
10	Configure VVB, on page 43 (optional)
11	Configure Cisco IOS Enterprise Voice Gateway, on page 43
12	Configure IPv6, on page 50

Sequence	Task
13	Configure Enterprise Chat and Email (ECE) (optional) Email and Chat

Configure CCE Component

Follow this sequence to configure components for Packaged CCE 12000 Agents deployment.

Sequence	Task
1	Configure SQL Server for CCE Components, on page 2
2	Set up Organizational Units, on page 2
3	Configure Logger, on page 112
4	Configure Router, on page 113
5	Configure AW-HDS, on page 113
6	Configure HDS-DDS, on page 113
7	Start Unified CCE Services, on page 64
8	If you have PG VMs installed , Add Unified CCE Instance, on page 76 on all PG VMs
9	Configure Packaged CCE Deployment Type, on page 67
10	Configure Cisco Unified Contact Center Enterprise PG, on page 77
11	For configuration using Configuration Manager, see Packaged CCE 4000 and 12000 Agent Supported Tools
12	For details on CA signed certificate, see *Generate and Import CA Signed Certificate in AW Machine*
13	For details on self-signed certificate, see Generate and Import Self-signed Certificate in AW Machine

Configure Logger

Follow this sequence to configure Logger for Packaged CCE 12000 Agents deployment.

Sequence	Task
1	Add Unified CCE Instance, on page 76
2	Create Logger Database, on page 60
3	To use Outbound Option, see Create Outbound Option Database, on page 61

Sequence	Task
4	Add Logger Component to Instance, on page 62
5	Cisco SNMP Setup, on page 21 (optional)

Configure Router

Follow this sequence to configure Router for Packaged CCE 12000 Agents deployment.

Sequence	Task
1	Add Unified CCE Instance, on page 76
2	Add Router Component to Instance, on page 63
3	Cisco SNMP Setup, on page 21 (optional)

Configure HDS-DDS

Follow this sequence to configure HDS-DDS for Packaged CCE 12000 Agents deployment.

Sequence	Task
1	Configure SQL Server for CCE Components, on page 2
2	Add Unified CCE Instance, on page 76
3	Create HDS Database, on page 64
4	Add Administration and Data Server Component to Instance, on page 65
5	Cisco SNMP Setup, on page 21 (optional)

Configure AW-HDS

Follow this sequence to configure AW-HDS for Packaged CCE 12000 Agents deployment.

Sequence	Task
1	Configure SQL Server for CCE Components, on page 2
2	Add Unified CCE Instance, on page 76
3	Create HDS Database, on page 64
4	Add Administration and Data Server Component to Instance, on page 65
5	Configure ICM Database Lookup, on page 114 (optional)
6	Cisco SNMP Setup, on page 21 (optional)

Configure ICM Database Lookup

You can use Database Lookup Explorer tool in Configuration Manager to view, define, delete, or edit script table from an external database.

Complete the following procedure to configure ICM Database Lookup.

Procedure

Step 1 Launch the Unified CCE Web Setup tool.

Step 2 In the Router Options window, select **Enable Database Routing**.

Step 3 Configure Database Lookup explorer:

a) Click **Start** > **All programs** > **Cisco Unified CCE Tools** > **Administration Tools** > **Configuration Manager**.

b) Open **Tools** > **Explorer Tools** > **Database Lookup Explorer.**

c) Configure Script Table and Script Table Column as shown in the following example:

Script Table:

```
Name: AccountInfo

Side A: \\dblookup1\DBLookup.AccountInfo

Side B: <Update Side B of database here>

Description: <Provide description here>
```

dblookup1 is external database server name, DBLookup is external database name, and AccountInfo is the table name.

Script Table Column:

```
Column name: AccountNo

Description: <Provide description here>
```

Step 4 Configure the following to change the registry settings in Unified CCE:

a) Navigate to **HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems, Inc. > ICM > <Instance Name> > RouterA > Router > CurrentVersion > Configuration > Database registry**.

Instance Name is the name of the Instance that is configured.

b) Set the SQLLogin registry key as shown in the following example:

Example:

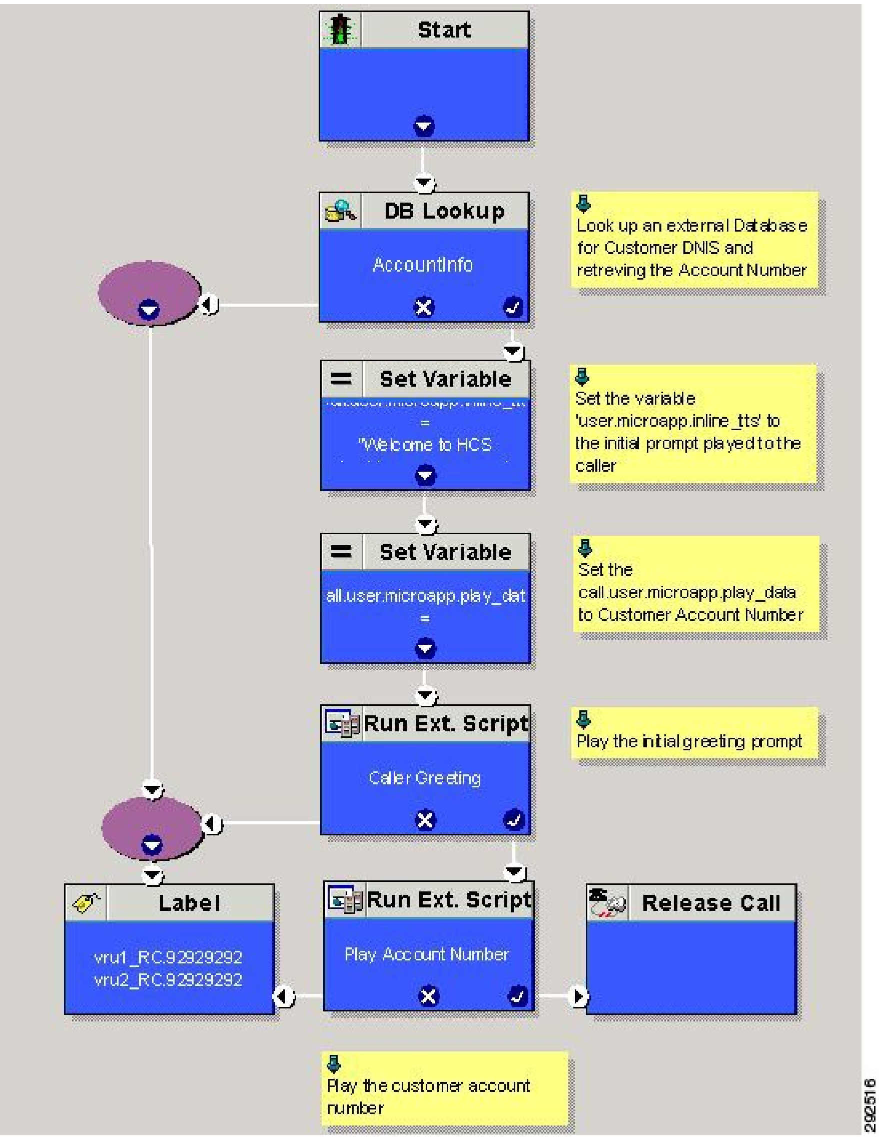
```
\\dblookup1\DBLookup=(sa,sa)
```

Where DBLookup is the external database name and (sa,sa) are the SQL server authentication.

Step 5 Create the ICM script with the database lookup node with the respective table and lookup value.

The following figure shows AccountInfo as the table name and Call.CallingLineID as the lookup value.

Figure 1: Example ICM Database Look Up


Start
DB Lookup
AccountInfo
Look up an external Database for Customer DNIS and retreving the Account Number
Set Variable
=
"Welcome to HCS
Set the variable 'user.microapp.inline_tts' to the initial prompt played to the caller
Set Variable
all.user.microapp.play_dat
=
Set the call.user.microapp.play_data to Customer Account Number
Run Ext. Script
Caller Greeting
Play the initial greeting prompt
Label
vru1_RC.92929292
vru2_RC.92929292
Run Ext. Script
Play Account Number
Release Call
Play the customer account number
292516

Packaged CCE Lab Only Deployments

Packaged CCE Lab Mode allows you to install Packaged CCE for demonstration and lab use. You can use all the features in a limited capacity without the need to install a full Packaged CCE deployment on supported hardware. If you exceed the capacity limit of an attribute, you are alerted with error messages that are displayed in **Unified CCE Administration**.

For procedures to configure and manage contact center operations using the Unified CCE Administration web-based tool, see Packaged CCE Administration.

The following Unified CCE Administration features are not initially available when you change into the Packaged CCE Lab deployment:

- System Inventory, available on the **Inventory** page
- Log Collection
- Live Data
- Single sign-on

Packaged CCE Lab Only Deployment Components

Packaged CCE Lab Mode allows you to install Packaged CCE for demonstration and lab use. You can use all the features in a limited capacity without the need to install a full Packaged CCE deployment on supported hardware. If you exceed the capacity limit of an attribute, you are alerted with error messages that are displayed in the **Unified CCE Administration** interface.

Packaged CCE Lab Only deployments can be configured as simplex systems or duplex systems only in 2000 Agents deployment. In a simplex system, all components are installed on Side A and there is no Side B. In a duplex system, components are installed on Side A and Side B.

Simplex Mode

The Lab Only simplex deployment must consist of the following components:

- 1 Unified CCE Rogger
- 1 Unified CCE AW-HDS-DDS
- 1 Unified CCE PG
- 1 Cisco Unified CM, functioning as a combined Publisher and Subscriber
- 1 Cisco Unified Intelligence Center, functioning as a combined Publisher and Subscriber
- 1 Cisco Finesse, functioning as both a Publisher and Subscriber
- Gateways
- SocialMiner
- Cisco MediaSense
- Cisco Enterprise Chat and Email
- Third-Party Multichannel

Note In the System Inventory, the status rules that apply to machines outside of the Packaged Contact Center Enterprise Simplex Lab Only deployment returns a status of blocked. Status rules which require ESXi host return a status of blocked.

For main site and remote site, you can add the following external machines:

- Cisco Virtualized Voice Browser

- Cisco Unified SIP Proxy
- Gateways
- MediaSense

Note: You can add MediaSense only for the main site.

- Cisco Unified CVP Reporting

Note: Adding a CVP Reporting Server via Inventory CSV is not supported. It can only be added as an external server after a successful initialization of inventory.

- Cisco Enterprise Chat and Email
- Third-Party Multichannel
- Media Server

Note: SocialMiner can be added as an external machine only in the main site.

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

Duplex Mode

The Lab Only duplex mode consists of the following components.

Note: In Lab Mode, Packaged CCE does not validate the ESXi host.

Side A

Side A must have the following:

- 1 Unified CCE Rogger
- 1 Unified CCE AW-HDS-DDS
- 1 Unified CCE PG
- 1 Cisco Unified CVP Server
- 1 Unified Communications Manager Publisher
- 1 Unified Communications Manager Subscriber

- 1 Unified Intelligence Center Publisher
- 1 Finesse Primary

Side B

Side B must have the following:

- 1 Unified CCE Rogger
- 1 Unified CCE AW-HDS-DDS
- 1 Unified CCE PG
- 1 Cisco Unified CVP Server
- 1 Unified Communications Manager Subscriber
- 1 Unified Intelligence Center Subscriber
- 1 Finesse Secondary

External

The Lab Only duplex mode can have the following external machines:

- Gateways
- Cisco Virtualized Voice Browsers
- Cisco Unified SIP Proxy
- SocialMiner
- Enterprise Chat and Email
- Unified CVP Reporting
- MediaSense
- third Party Multichannel
- Media Server

Note Status rules which require ESXi host returns a status of blocked.

For remote site, you can add the following external machines:

- Cisco Unified CVP Reporting
- Cisco Enterprise Chat and Email
- Third-Party Multichannel
- Media Server

Note SocialMiner can be added as an external machine only in the main site.

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

Initialize the Packaged CCE Lab Mode Deployment

When you sign into Unified CCE Administration for the first time, you are prompted to supply information and credentials for the components in your deployment. Packaged CCE uses this information to configure the components and build the System Inventory.

Procedure

Step 1 On the **Inventory** page, select **Packaged CCE: Lab Mode** from the **Deployment Type** drop-down list, then select an instance from the **Instance** drop-down list that has been created using Domain Manager. Click **Next**.

Step 2 Select one of the following options from the **Template** drop-down list:

- Simplex Inventory for Simplex Lab Mode deployment
- Duplex Inventory for Duplex Lab Mode deployment

Click **Download** to download the Inventory Content File Template. Fill out and save the template to your computer. In the required **Content File** field, browse to the content file you have completed. The content file is validated before the inventory is created. Click **Next**.

For more information on completing the Inventory Content File Template, see Inventory Content File , on page 121.

Step 3 On the **Settings** page do the following:

- Select the codec used for Mobile Agent calls from the **Mobile Agent Codec** drop-down list. The **Side A Connection** and **Side B Connection** drop-down lists are disabled in Lab Only deployment.
- For the **Automatically create service accounts** check box, either:
  - Uncheck the check box if you want to use an existing Active Directory account. Enter the username and password for an existing Active Directory user in the same domain as the Packaged CCE servers.

    This account will be added to the Service group.

Click **Next**.

The deployment is initialized. The **Details** dialog box displays the status of the automated initialization tasks.

Step 4 After the automated initialization tasks complete, click **Done**.

If one of the automated initialization tasks fails, correct the errors and then click **Retry**.

If the retry is successful, the automated initialization continues.

For some task failures, all completed tasks must be reverted before the task can be retried. You see a message informing you that the system needs to be reverted to a clean state.

Click **OK**, and then after the system is in a clean state, click **Start Over**.

Note You should restart the Unified CVP Server.

After you initiate Simplex or Duplex Lab Mode deployment, you can also add the following external machines for the main site on the **Inventory** page:

- Unified CM Publisher
- Unified CVP Reporting Server
- Unified SIP Proxy
- Virtualized Voice Browser
- Gateway
- SocialMiner
- MediaSense
- Enterprise Chat and Email
- Third-party Multichannel
- Media Server

To add, edit or delete the external machines on the main site, see System Inventory for Packaged CCE 2000 Agents Deployment, on page 9.

Enable System Inventory, Log Collection, and Live Data Using the Inventory Content File

To use the following Unified CCE Administration features for demonstration purposes, you must provide Packaged CCE with information and credentials for the machines in your deployment:

- System Inventory (available under **Inventory** page)
- Log Collection
- Live Data
- Single Sign-on

You provide this information using the Inventory Content File.

If you are configuring the Packaged CCE Lab Only deployment in Unified CCE Administration as part of the installation process, you are prompted to complete and upload the Inventory Content File.

If you switch into Packaged CCE Lab Only deployment from a different deployment, you complete and upload the Content Inventory file in Unified CCE Administration from the Bulk Importtool.

To complete and upload the Content Inventory file in Bulk Import:

Procedure

Step 1 In the Unified CCE Web Administration, click the **Bulk Import** card on the **Overview** page. Download the Inventory content file template.

Step 2 Open the file in Microsoft Excel and populate the content file fields as described in Inventory Content File.

Step 3 Save your changes.

Step 4 Create a new bulk job in **Bulk Jobs**. In the **Content File** field, select the Inventory content file you created and click **Save**.

Related Topics

Manage Bulk Jobs

Inventory Content File

The Inventory content file template contains the following fields:

Note If a username and/or password contains the "=" or "&" characters, use the encoded value of "%3D" or "%26" respectively.

Field	Description
operation	The default is CREATE; do not change the operation.
name	Do not change the machine name. **Note** This field applies only to duplex mode.
machineType	Do not change the machine type.
publicAddress	Enter the public IP address or hostname for each machine.

Field	Description
publicAddressServices	**CCE_ROGGER** - Do not change this field. **CCE_PG** - This field specifies services that are required for the Unified CCE PG. If the Logical Controller ID for the UCM PG is not the default of 5000, change the pairing value for the TIP_PG and TIP_PG_TOS services to match the Logical Controller ID. (The Logical Controller ID can be found on the Peripheral Gateways tab of System > Information.) **CCE_AW** - Unified CCE Diagnostic Framework Portico domain, username, and password. These credentials must be of a domain user who is a local administrator on all the CCE servers and valid on all Unified CCE components in your deployment (the Side A and Side B Unified CCE Roggers, PGs, and AW-HDS-DDSs). **Note** Every time the Active Directory credentials are updated, the credentials configured here must be updated as well. **CVP** - Unified CVP Server Windows credentials **CM_PUBLISHER** - This field specifies AXL credentials. Replace user and password with the correct credentials. **CUIC_PUBLISHER** - This field specifies the services for Unified Intelligence Center. For the Administration credentials and Cisco Identity Service credentials, replace user and password with the correct credentials. For all other services, do not change the default values. **FINESSE** - This field specifies Finesse Administration credentials. Replace user and password with the correct credentials.
privateAddress	Enter the private IP address for the **CCE_PG** and **CCE_ROGGER**. Leave this field blank for all other machines.
side	Enter sideA or sideB.