Initial Configuration

Initial Configuration Overview

This initial configuration brings the contact center to the point where a complete call flow is possible. The configured system will process information about incoming calls, perform call routing, and enable call handling.

Initial Configuration Task Flow

Task	See
Set Deployment Type in Unified CCE Administration Configuration	Set Deployment Type in Unified CCE Administration Configuration
Configure Cisco Unified Contact Center Enterprise	Configure Cisco Unified Contact Center Enterprise, on page 3
Configure Cisco Unified Intelligence Center	Configure Cisco Unified Intelligence Center, on page 43
Configure Cisco Unified Customer Voice Portal	Configure Cisco Unified Customer Voice Portal, on page 50
Configure Cisco Unified Communications Manager	Configure Cisco Unified Communications Manager, on page 68
Configure Cisco Finesse	Configure Cisco Finesse, on page 78

Initial Configuration Tasks

Configure Permissions in the Local Machine

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

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

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

Configure Registry Permissions

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

Procedure

Step 1 Run the `regedit.exe` utility.

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

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

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

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

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

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

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

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

Configure AW-HDS Database Permissions

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

Procedure

In SQL Management Studio, do the following:

a) Go to **Security** > **Logins**.
b) Locate `<Machine netbios name>\UcceConfig`. Right-click and select properties.
c) Go to **User Mappings** and select one AWDB database. Ensure that GeoTelAdmin, GeoTelGroup, and public are selected.
d) Repeat step c for the HDS database.

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

Configure Folder Permissions

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

Procedure

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

What to do next

To establish secure connection between a client and a server, use one of the following security certificates:

Configure Cisco Unified Contact Center Enterprise

You can configure individual records, or you can use the Bulk Configuration tool to configure multiple records at one time. Bulk configuration is available for the following:

- Agents
- Call types
- Dialed number plans
- Dialed numbers
- Labels

- Network trunk groups
- Network VRU scripts
- Peripheral targets
- Persons
- Regions
- Region prefixes
- Routes
- Trunks
- Trunk groups
- Scheduled targets
- Services
- Skill groups
- VRU port maps

Access Configuration Manager tool

You perform all Unified CCE configuration tasks using the Configuration Manager tool, which is installed with the Unified CCE software.

1. From your desktop, double-click the Unified CCE Tools icon, and then select Administration Tools.
2. Double-click the Configuration Manager icon.

Configure Media Routing Domain

You must establish Media Routing Domains (MRD) for each media type that your Unified CCE System supports. A Voice MRD is installed by default with Unified CCE. You need to create MRDs for other media such as chat, email, and tasks. Additionally, if you are using Cisco Enterprise Chat and Email (ECE), you need to create media classes for ECE chat and email.

If you are configuring Media Routing Domains for ECE, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* for complete instructions, at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Important If you are configuring a Media Routing Domain for Task Routing with third-party multichannel applications, do not use this procedure. See the *Cisco Unified Contact Center Enterprise Features Guide* for instructions, at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

Procedure

Step 1 Start the Configuration Manager and select **Tools** > **List Tools** > **Media Routing Domain List**.

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

The Attributes tab appears.

Step 3 On the Attributes tab, provide values for the following fields:

Name. Enter the enterprise name of the MRD.

Media Class. Use the drop-down list to select the media class for the integrated application.

Max Time in queue. The default maximum queue time for calls in queue is one hour. To override this default, modify the value of the Max Time In queue field.

The MR domain ID is automatically generated when you save the MRD.

Step 4 After completing the required fields, click **Save**.

Repeat this procedure to add an MRD for each media class that your system supports.

Configure Trunk Groups

For the Unified CCE, the *Network Trunk Group* is the placeholder in the Unified CCE database for the trunk group; it performs no other function.

For deployments that:

- Use the Unified CCE System PG, you must create one Network Trunk Group for each Unified CCE System PG peripheral.
- Do not use the Unified CCE System PG, you must create two Network Trunk Groups—one for the Unified Communications Manager and one for the Unified CVP or Unified IP IVR. If you are deploying the Unified CVP, create one Network Trunk Group per CVP Server.

A Unified CCE *Trunk Group* is a collection of trunks associated with a single peripheral and usually used for a common purpose. For the Unified CCE, the trunk groups for VRU peripherals are used primarily as a place holder in the Unified CCE database.

Create a trunk group for each Unified Communications Manager peripheral and a trunk group for each Unified IP IVR application. If you are deploying Unified CVP, you must create two trunk groups for each Unified CVP Server that match the Group Numbers configured in Unified CVP Application Administration. For Unified IP IVR, the trunk group peripheral number in the Unified CCE must match the CTI Port Group ID on Unified IP IVR.

To configure a Network Trunk Group (and the trunk group under it):

Procedure

Step 1 From the Configuration Manager, choose **Configure ICM** > **Peripherals** > **Trunk Group** > **Network Trunk Group Explorer**. The ICM Network Trunk Group Explorer dialog box opens.

Step 2 Click **Retrieve**.

Step 3 Click **Add Network Trunk Group**. The Network Trunk Group tab opens.

Step 4 Add a unique name for the Network Trunk Group and an appropriate description.

Step 5 Click **Add Trunk Group** to add a trunk group.

Step 6 Complete these fields:

Peripheral. Select the peripheral to which the trunk group is associated.

Peripheral Number. Enter the number of the trunk group as understood by the peripheral. This number must be unique among all trunk groups associated with the peripheral. For Unified IP IVR, this number must:

a. Match a CTI Port Group ID configured on the Unified IP IVR.

b. Be an odd number.

c. Be unique for all Unified IP IVRs handled by an Unified CCE System PG.

For example, if a Unified CCE System PG handles four Unified IP IVRs and each Unified IP IVR peripheral has one CTI Port Group, then the CTI Port Group ID for the first Unified IP IVR should be 1, the port group ID for the second Unified IP IVR should be 3, and so on. For the Unified CVP, this number must match a CVP Server Group Number configured on the CVP Server.

Peripheral Name. Enter the name of the trunk group as understood by the peripheral. This name must be unique among all trunk groups associated with the peripheral.

Name. Enter the enterprise name of the trunk group. The Unified CCE forms a default for this name using the entries from the Peripheral and Peripheral Name fields.

Extension. Leave this field blank.

Trunk Count. Select **Use Trunk Data**. When you specify **Use Trunk Data**, the system software determines the trunk count dynamically by counting the associated records in the Trunk table.

Configuration Parameters. Leave this field blank.

Description. Enter an optional description.

Step 7 To add trunks to the trunk group, click **Add Trunk**.

Step 8 Add trunks as desired.

Step 9 Click **Save** and then click **Close**.

Step 10 Repeat these steps to create all necessary trunk groups.

Configure Network VRU Bank

The *Network VRU Bank* allows load balancing across multiple VRUs to occur and eliminates the need for complex translation-route configuration.

Configure a Network VRU Bank, only if your deployment uses the Unified CCE System PG.

Before you begin

Do this after you configure the following:

- Network VRU
- Network Trunk Group

- All other trunk groups

Procedure

Step 1 From the Configuration Manager, choose **Explorer Tools** > **Network VRU Explorer**. The Network VRU Explorer dialog box opens.

Step 2 Click **Retrieve** and select your Network VRU.

Step 3 Select the Network VRU Bank tab and click **Add**.

The Select Trunk Group dialog box opens, displaying the all trunk groups configured on all Unified CCE System PG peripherals.

Step 4 Select the trunk group associated with the translation routing group on your Unified IP IVR. Make the appropriate trunk group selection for each Unified IP IVR in your deployment.

Step 5 Click **OK**.

Step 6 Click **Add Label** to add a label for the Network VRU Bank. The label must be the CTI Route Point trigger for the Translation-Routing application on the Unified IP IVR. By default, in the Label tab, the first field shows the selected Network VRU, *not* the Network VRU Bank:

a) Click the drop-down list box to show the available Network VRU banks.
b) Select a Network VRU bank in the drop-down list.
c) Then configure the label for the Network VRU bank.
d) Repeat the steps to configure labels for all of the Network VRU Banks.

If Network VRU Bank labels are available, the Router uses them when it balances the load between the Unified IP IVRs. If the Router cannot find an eligible Network VRU Bank labels, it uses the Network VRU label.

Configure services

A *service* refers to a type of processing that a caller requires. For example, separate services might be defined for Sales, Support, or Accounts Payable. Services are often associated with a peripheral, and are sometimes referred to as peripheral services. An agent is assigned one or more skills that in turn is associated with services. Routing to a Unified CCE service effectively targets an agent assigned to a Unified CCE skill group associated with the Unified CCE service.

Services on the Unified CCE correspond to CTI Route Points on Unified Communications Manager.

Note On Unified CCE systems that interface with Unified CVP systems, you *must* configure two services with Peripheral Numbers of 1 and 2. However, outside of these services the preferred method of defining Unified CCE routable tasks is by defining call types.

For the two Unified CVP services, you do not need to configure Service Members, Routes, Peripheral Targets, or Labels.

Procedure

Step 1 From the Configuration Manager menu, choose **Tools** > **Explorer Tools** > **Service Explorer**. The Service Explorer dialog box opens.

Step 2 Select the peripheral for which you want to create a service and click **Retrieve**.

Step 3 Click **Add Service**.
The Service Configuration window opens.

Step 4 On the Service tab, enter the following:

The **Media Routing Domain** associated with the service.

Peripheral Number. Enter the number for the service on the peripheral. This field must be unique for all services for the peripheral, but not necessarily across all peripherals. If you are deploying the Unified CVP, enter 1 for the first service and 2 for the second service.

Peripheral Name. Enter a name that describes the service.

Enterprise Name. Enter an enterprise name for the service. This name must be unique among all the services in the enterprise. If you do not enter a value, this name is autogenerated.

Config Param. Not used for the Unified CCE.

Description. Enter any additional information about the service.

Service Level Type. Indicates how the Unified CCE calculates the service level for the service. You can choose to omit abandoned calls from the calculation, treat them as having exceeded the threshold (negative impact on service level), or treat them as answered calls (positive impact on service level). You can also choose to use the default specified for the peripheral.

Service Level Threshold. Enter the time in seconds, for the service level. The Unified CCE tracks the percentage of calls answered within this threshold. If this field is negative, the value of the default for the peripheral is used.

Step 5 On the Advanced tab, enter the following:

Peripheral Service Level. Indicates the type of service level calculation that the peripheral performs for this service. This setting has no effect because the PG does not report a peripheral service level.

Schedule name. Identifies an imported schedule associated with the service.

Extension. If you are deploying Outbound Option, enter the extension to associate with this service. This corresponds to a CTI Route Point defined in Unified Communications Manager and is associated with the PG User.

Step 6 On the Service Members tab, select skill groups to associate with this service.

Step 7 Click **Apply**.

Step 8 Repeat this procedure to add any other services.

Configure dialed numbers

The *dialed number* (DN) is the number that the caller dials to start the call and identifies the Unified CCE routing script to run. Set dialed numbers for ring no answer, dialed number plan entries, and for Supervisor/emergency calls.

For Unified Communications Manager to generate a route request to the Unified CCE, the cluster associates the DN with a CTI Route Point for the Unified CCE JTAPI User. Configure the DN in the Unified CCE. After the Unified CCE receives the route request with the DN, that DN is mapped to a Unified CCE Call type, which is then mapped to a Unified CCE routing script.

Note You cannot use the DN for a CTI Route Point on a different CTI Route Point in another partition. Ensure that DNs are unique across all CTI Route Points on all partitions.

Unified CCE generates a unique value for the Label Name list after you configure a dialed number.

Procedure

Step 1 From the Configuration Manager, choose **Tools > List Tools > Dialed Number/Script Selector List**.

The Dialed Number/Script Selector List dialog box opens.

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

The Attributes tab displays.

Step 3 In the Attributes tab, enter values in the following fields:

Routing client. Choose the enterprise name of the routing client associated with this dialed number. After you select a routing client and save to the database, this field becomes read only.

Media Routing Domain. The media routing domain associated with the selected dialed number or script selector.

Dialed number string. Enter the string value that the routing client passes to the Unified CCE for this dialed number (for example: 8005551212).

Name. Enter the enterprise name for the dialed number. This name must be unique among all dialed numbers in the system. If you do not enter a value, the name is autogenerated.

Customer. Use the drop-down list to select the customer (Unified CCE instance) associated with the dialed number.

Default label. Choose the name of the default label for this dialed number. The label must have been previously defined for it to be in the selection list. Use the Label List tool in the Configuration Manager to define labels. If the Unified CCE fails to determine a target for the call within the routing client's time-out threshold, then the default label for the dialed number is used.

Description. Enter a description for the dialed number.

Permit application routing. If you intend to route calls from a parent system to this dialed number, check this dialog box.

Reserved by IVR. For VRU dialed numbers, check this box. This setting prevents the CallManager PIM from trying to exert control on the calls arriving on these Route Points.

Step 4 On the DN Mapping tab, as desired, click **Add** to specify a call type and other dialing information to associate with this dialed number.

Step 5 Click **Save** to enter the dialed number information.

Step 6 Repeat this procedure for any additional dialed numbers.

Configure call types

A *call type* is a category of Unified CCE routable task. Each call type has a schedule that determines which routing script or scripts are active for that call type at any time.

There are two classes of call types:

- Voice (phone calls). Voice call types are categorized by the dialed number (DN), caller-entered digits (CED), and calling line ID (CLID). The CED and CLID can be optional, depending on the call.
- Non-voice (email and text chat). Non-voice call types are categorized by the Script Type Selector, Application String 1, and Application String 2. Application String 1 and Application String 2 can be optional, depending on the application.

To facilitate Unified CCE reporting, it is good practice to create separate call types for VRU applications and queuing applications.

Procedure

Step 1 From the Configuration Manager, select **Tools** > **List Tools** > **Call Type List**.

The Call Type List dialog box opens.

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

The Attributes tab appears.

Step 3 In the Attributes tab, enter values for the following fields:

Name. Enter an enterprise name for the call type. This name must be unique among call types in the system.

Customer. Choose the customer (Unified CCE Instance) from the drop-down list.

Service level threshold. The service level threshold is the target maximum time that a caller spends in a queue before being connected to an agent. When you set up a peripheral, you specify a default service level threshold for all services associated with that peripheral. If you enter a negative number, the service level threshold from the Peripheral table is used.

This field is prepopulated with the default service level threshold for this peripheral and grayed out. If you wish to override this default, check the **Override System Information Default** check box to the right of this field and enter a different value.

You can also set the Service Level in the Configuration Manager with the System Information tool. When the service level is defined with the Call Type tool, this setting overrides a setting made with the System Information tool. If service level is not defined with the Call Type tool, but is defined with the System Information tool, the Unified CCE uses the System Information setting.

Service level type. Indicates how the system software calculates the service level for the service. The default is the level specified for the associated peripheral. To set a different level type, check the **Override System Information Default** check box and select the type you want from the selection box.

Bucket Intervals. Indicates the Bucket Intervals setting for the call type. Bucket intervals are defined with the Bucket Intervals List tool. If you wish to override the defined default, check the **Override System Information Default** check box and select a different Bucket Intervals setting.

Description. Enter an optional description of the call type.

Step 4 Click **Save** to enter the call type information.

Repeat this procedure to add additional call types.

Configure Variables

Configure Expanded Call Context Variables

Expanded Call Context (ECC) variables are variables that you define and enable in the Configuration Manager to store values for a call. You can specify the variable name and data type. The name must begin with the string "user." ECC variables are in addition to the variables the system software defines for each call (PeripheralVariable1 through PeripheralVariable10, CallerEnteredDigits, CallingLineID, and so on).

An ECC variable name can be up to 33 bytes long (1–32 usable characters). Use the following naming convention when creating an ECC variable:

user.<CompanyName>.<VariableDescription>

In this syntax:

- **<CompanyName>** is the name of your company.
- **<VariableDescription>** is a descriptive tag for the variable.

For example:

```
user.Cisco.AcctNum
```

Using this naming convention prevents naming conflicts with any third-party applications that interface with the system software.

Note For a large corporation, you can break **<VariableDescription>** down to include the Business Unit, Division, or other organizational entities.

ECC variables follow these size rules:

- An ECC variable can be either a scalar variable or an array element, each with a maximum length of 210 bytes.

Note Array types are not supported for an agent request.

- The maximum number of elements in an array is 255.
- The maximum buffer size for each scalar variable = 5 + the maximum variable length. The 5 bytes includes 4 bytes to tag the variable and 1 byte for the null terminator.

- The maximum buffer size for each array = 5 + (1 + the maximum length of an array element) * (the maximum elements in the array). There is a null terminator for each element, and a null terminator for the array as a whole.
- You pass ECC variables in an ECC payload which has a 2000-byte limit. The total sum of all the maximum buffer sizes for each variable and each array in one ECC payload cannot exceed 2000 bytes.

  For example, if you intended to use the following:

  - A scalar ECC variable with a maximum length of 100 bytes
  - A scalar ECC variable with a maximum length of 80 bytes
  - An ECC array with a maximum of 9 elements with each element having a maximum length of 200 bytes

  Totaled the buffer size is: (5+100) + (5+80) + (5 + (1+200)*9) = 2004. Because this size is too large, you must change the length of one of the scalar ECC variables or the length of the array ECC variables.

For Web Callback and Delayed Callback to work properly, an ECC variable (also known as a named variable) must be defined. The Cisco CTI driver supports the use of ECC variables in addition to the standard call variables associated with a call. Before an ECC variable can be used, it must be defined in the Unified CCE ECC variable database table.

ECC Variables for Voice MRDs with Collaboration

ECC variables must be configured in Configuration Manager's Expanded Call Variable List tool (for each integrated application) to route requests using the voice Media Routing Domain.

For Voice MRDs with Collaboration, the ECC variables are:

- user.ewm.activity.id
- user.ewm.customer.name

Validate ECC Variable Size for CTI Server

Before configuring ECC variables, validate the total size of the ECC variables against the following rules and limits:

- Because the total size of the buffer used to store the variables in CTI Server internally is 2500 bytes, the total sum of all the maximum buffer sizes for each scalar variable and arrays must be no greater than 2500.
- The maximum buffer size for each scalar variable = 4 + length of the ECC name + the maximum length of the variable where the 4 bytes includes a 1 byte tag, 1 byte to define the length, and 2 terminating NULL characters.
- The maximum buffer size for each array = (5 + length of the ECC name + the maximum length of array element) * (the maximum number of elements in the array) where the 5 bytes includes a 1 byte tag, 1 byte to define the length, 1 byte for the array index, and 2 terminating NULL characters.
- For example, if you intend to use one scalar ECC variable with a maximum length of 100 bytes named *user.var*, one scalar ECC variable with a maximum length of 80 bytes named *user.vartwo*, and an ECC array named *user.varthree* with a maximum of 9 elements with each element having a maximum length of 200 bytes, the buffer size would be:

(4+8+100) + (4+11+80) + ((5 + 13 + 200)*9)) = 2169

where 8 is the length of *user.var*, 11 is the length of *user.vartwo* and 13 is the length of *user.varthree*.

Enable ECC Variables

Procedure

Step 1 Within the Configuration Manager, double-click **Tools** > **Miscellaneous Tools** > **System Information**.

The System Information window appears.

Step 2 Select the **Expanded call context enabled** check box.

For additional information, refer to the online Help.

Step 3 Click **Save** to apply your changes.

Define ECC Variables

Procedure

Step 1 Within the Configuration Manager, double-click **Tools** > **List Tools** > **Expanded Call Variable List**.

The **Expanded Call Variable List** window appears.

Step 2 Click **Retrieve** to enable adding ECC variables.

Step 3 Click **Add**.

The **Attributes** property tab appears.

Step 4 Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.

Step 5 Click **Save** to apply your changes.

What to do next

If you change the configuration of any ECC variable with the **Expanded Call Variable List** tool, restart the Unified CVP Call Server or VRU PIM to force a renegotiation of the ECC variables.

Before you can use the new ECC variable, you must add it to an ECC payload.

Note If your solution only has a Default payload, the solution automatically adds any new ECC variables to the Default payload until it reaches the 2000-byte limit.

Define ECC Payloads

You can create and modify ECC payloads in the **Expanded Call Variable Payload List** tool.

Note The tool checks that the ECC payload does not exceed the 2000-byte limit only when you save your changes. The counters on the **Members** tab only show what the current size is with all the selected members. They are only informational and do not enforce the limit. The limit is enforced when you attempt to save the changes.

To define an ECC payload, you create the ECC payload and then add its members.

Procedure

Step 1 In the Configuration Manager, open **Tools** > **List Tools** > **Expanded Call Variable Payload List**.

The **ECC Payload List** window appears.

Step 2 Click **Retrieve** to enable adding ECC payloads.

Step 3 Click **Add**.

The **Attributes** property tab appears.

Step 4 Complete the **Attributes** property tab. See the *List Tools Online Help* for details on the **Attributes** property tab.

Step 5 On the **Members** tab, click **Add**.

A dialog box listing all the existing ECC variables appears.

Step 6 Select the members for your ECC payload and click **OK**.

Watch that the **ECC Variable Size** counter does not exceed 2000 bytes. For ECC payloads that go to CTI clients, watch that the **CTI Message Size** counter does not exceed 2500 bytes.

Step 7 Click **Save** to apply your changes.

Configure User Variables

You can also create global user variables; for example, you can create a user variable called usertemp to serve as a temporary storage area for a string value used by an If node.

After you have defined a user variable, you can then use the Script Editor Formula Editor to access the variable and reference it in expressions, just as you would with a “built-in” variable.

Each user variable must:

- Have a name that begins with **user**.

Note This name cannot contain the dot/period (.) character.

- Be associated with an object type, for example, Service. (This enables the system software to maintain an instance of that variable for each object of that type in the system.)
- Be checked as persistent. A persistent variable maintians its value between script invocations. This allows you to set the variable in one script and reference later in another script.

Note Because these variables may be persisted, do not use User Variables to store sensitive information belonging to the customer or company. Using these variables to store confidential information could lead to violation of security standards, such as PCI, the Common Criteria, HIPAA, or FIPS 140-2.

A user variable can store a value up to 40 characters long.

Define User Variables

Procedure

Step 1 Within the Configuration Manager, select **Tools** > **List Tools** > **User Variable List**.

The User Variable List window appears.

Step 2 In the User Variable List window, click **Retrieve** to enable Add.

Step 3 Click **Add**.

The Attributes property tab appears.

Step 4 Complete the Attributes property tab.

Note The **Variable name**, **Object type**, and **Data type** fields are required. All other fields are optional. For additional information refer to the online Help.

Step 5 Click **Save** to apply your changes.

Configure Users

Create Person records

All Unified CCE agents must have a *Person* record. When you create an Agent record, you can associate the record with an existing Person record. If you do not associate the Agent record with an existing Person record, a new Person record is automatically created when you create the agent.

To configure a Person record before configuring an agent, complete the following steps:

Procedure

Step 1 From the Configuration Manager, choose **Peripherals** > **Person** > **Person List**.
The Person List dialog box opens.

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

Step 3 in the Attributes tab, enter information in the following fields:

First Name. Enter the person's first name.

Last Name. Enter the person's last name.

Login Name. Enter the person's login name.

Password. Enter a password for the person.

Enable Logins. Check this check box.

Step 4 Click **Save** and then click **Close**.

Step 5 Repeat this procedure to add additional Person records.

Associate agents with peripherals

Procedure

Step 1 Select **Tools** > **Explorer Tools** > **Agent Explorer**.
The Agent Explorer dialog box displays.

Step 2 Select the peripheral you want associated with the agent from the drop-down list and click **Retrieve**.

Step 3 Click **Add Agent** to display the Agent configuration tab.

Step 4 In the Agent tab, enter information in the following fields:

Last Name. Enter the agent's last name.

First Name. Enter the agent's first name.

Login Name. Enter the name the agent uses to login. This name must be unique in the enterprise.

Password. Enter the agent's password. This password is validated during the agent login process.

Login Enabled. Check this check box if you want the enable the agent to login.

Select Person. Click this button to select a person to associate with the agent record. You can select a person for a new agent, an existing agent, or a temporary agent.

Enterprise Name. Enter an enterprise name for the agent that is unique within the enterprise. The default is a combination of the peripheral name with the agent's first and last name.

Peripheral Name. Enter a name for the agent as known to the peripheral.

Peripheral Number. Enter the agent's login ID. This number identifies the agent to the peripheral. This number needs to be unique among all agents for the peripheral, but does not need to be unique across all peripherals. Agent IDs can be up to eleven digits long. The first digit in the ID must be 1 through 9. It cannot be 0. Also, this number cannot be the same as the extensions on the Unified Communications Manager cluster for this agent. Finally, the ID can not exceed the extension length specified in the Unified Communications Manager Peripheral Gateway Setup

Step 5 Click the Advanced tab and enter information in the following fields:

Desk Setting. Use the drop-down list to select the desktop settings to be associated with the agent. If you do not make a selection, the Unified CCE applies the default desk settings defined for the peripheral.

ConfigParam. Use this field to enter any specific configuration parameters that may be required. Make entries in this field only if instructed to do so by your Cisco support representative.

Description. Enter any other information you want about the agent.

Agent State Trace. Select to enable the agent's state trace control. When enabled, the Unified CCE records every state transition made by the agent.

Step 6 Click **Save**.

Step 7 Repeat this procedure to configure additional agents.

Assign Agent Desk Settings

Agent Desk Settings associate a set of permissions or characteristics with specific agents. The settings are comparable to Class of Service settings on a PBX or ACD. Desk settings are associated with an agent when you configure the agent. The desk settings are global in scope and you can apply them to any configured agent on any peripheral within a Unified CCE configuration.

Agent Desk Settings provide a profile that specifies parameters such as whether auto-answer is enabled, how long to wait before rerouting a call for Ring No Answer, what DN to use in the rerouting, and whether reason codes are needed for logging out and going not-ready. You must associate each agent with an agent desk setting profile in the Unified CCE configuration. A single agent desk setting profile can be shared by many agents. Changes made to an agent's desk setting profile while the agent is logged in are not activated until the agent logs out and logs in again.

If Agent Desk Settings are not associated with an agent, the agent is assigned the peripheral default settings, which depend on the peripheral to which the agent is assigned.

When you configure Agent Desk Settings, you specify the amount of non-active time after which an agent is automatically logged out, whether wrap up is required following incoming and outbound calls, the amount of time allocated for wrap up, and the method used for assist and emergency calls. You also specify settings for the Ring No Answer feature.

Ring No Answer

The Ring No Answer feature, configured in Agent Desk Settings, ensures that when an agent does not answer a call, the call is taken away from the agent after a specified number of seconds and re-assigned to another agent or requeued.

When a call is routed to an agent but the agent fails to answer the call within a configurable amount of time, the Unified Communications Manager PIM for the agent who did not answer changes that agent's state to not ready (so that the agent does not get more calls) and launches a route request to find another agent. Any call data is preserved and popped onto the next agent's desktop. If no agent is available, the call can be sent back to the Unified IP IVR for queuing treatment again. Again, all call data is preserved. The routing script for this RONA treatment should set the call priority to “high” so that the next available agent is selected for this caller. In the agent desk settings, you can set the RONA timer and the DN used to specify a unique call type and routing script for RONA treatment.

This feature behaves and is configured differently depending on whether you deploy the Unified CVP or Unified IP IVR in the Unified CCE System.

Note The Dialed Number for Ring No Answer is peripheral-specific. Therefore, each Unified Communications Manager PG in your deployment must have its own set of Agent Desk Settings configured for it; you cannot use a particular desk setting across peripherals.

About Ring No Answer with Unified IP IVR

For Unified CCE systems in which you deploy the Unified IP IVR, the Ring No Answer feature ensures that when an agent does not answer a call the following applies:

- The call is taken away from that agent after ringing for a configurable number of seconds and is rerouted to a different agent or placed in queue.
- The state of the agent who did not answer the call is changed to “Not Ready.”

Reroute a call on Ring No Answer works as follows for Unified IP IVR:

1. A routing script connects the call to an agent.
2. If the agent does not answer the phone within the Ring No Answer time set in Agent Desk Settings, the Unified Communications Manager changes the agent's state to “Not Ready” and post routes the call to Unified CCE.
3. The Unified CCE Router runs a routing script using the dialed number specified in the agent desk setting record. The routing script associated with the DN typically looks for another agent and routes the call to that new agent.
4. If no agents are available, the call typically is translation routed or queued to the VRU, or sent to some other queue point. Queuing treatment is restarted.

Note Give the call the highest priority in the queue so that the call is routed to the next available agent.

5. Any call data is preserved to be popped onto the agent screen. In addition, a flag is set in the database so that Unified CCE can report on all of the occurrences of Ring No Answer.

About Ring No Answer with Unified CVP

For Unified CCE systems in which you deploy the Unified CVP, the Unified Communications Manager does not control the Unified CVP and cannot send an unanswered call back to the Unified CVP for re-queuing. You configure the Ring No Answer feature to only make the agent “Not Ready” when they do not answer a call, and use the Unified CVP Router Requery feature to re-queue the call.

As of Release 9.0, the Unified CVP deployment no longer requires that you configure the RNA timer on both sides (Unified CVP and Unified CCE); configure Ring No Answer (RNA) timeout only in Unified CVP. This removes the requirement to manually align the relevant Unified CVP and Unified CCE timer configuration. To configure RNA timeout in Unified CVP, see the **Patterns for RNA timeout on outbound SIP calls** section in the Unified CVP OAMP console.

Reroute a call on Ring No Answer works as follows for Unified CVP:

1. A routing script connects the call to an agent by sending a connect message to the Unified CVP. The script node should have Enable Target Requery enabled. To enable this, edit the node, select **Change** and check the **Enable Target Requery** check box.
2. The agent's phone rings.
3. If the phone is not answered (either via the agent desktop or physically going off-hook) within the Ring No Answer time set in Agent Desk Settings, Unified CCE makes the agent unavailable, but does not actually change the agent state to Not Ready until the call is redirected.

4. When the Unified CVP Ring No Answer timeout expires, the Unified CVP sends an EventReport=No Answer message to the Router instructing it to select another target according to the routing script and send a Connect message to Unified CVP. The target might be another agent or a VRU label to requeue the call.

Note Give the call the highest priority in the queue so that the call is routed to the next available agent.

5. Any call data is preserved to be popped onto the second agent screen.

Note In addition, a flag is set in the database so that Unified CCE can report on all of the occurrences of Ring No Answer.

6. When the call is redirected from the original agent, the agent's state changes to “Not Ready.”

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.

Designate Agent Supervisor

You can identify an agent as a supervisor.

If you define an agent as a supervisor:

- If single sign-on is *disabled* either globally or for the agent you want to designate as a supervisor, the supervisor must have an Active Directory account. If the supervisor does not have an Active Directory account, the designation fails.
- If single sign-on is *enabled* either globally or for the agent you want to designate as a supervisor, you must enter the individual's name in the format that your identity provider requires.

To create an agent who is a supervisor:

Procedure

Step 1 In the Configuration Manager menu, select **Tools** > **Explorer Tools** > **Agent Explorer**. The Agent Explorer window appears.

Step 2 In the **Select filter data** box, select the peripheral with which the agent is to associated and click **Retrieve**. This enables the **Add Agent** button.

Step 3 Click **Add Agent**.

Note You must add the agent supervisor, as both member and supervisor, to the **Member** tab on the agent team list. To get the benefit from the Team layout in Finesse, the agent supervisor must be a member of the team.

Step 4 In the property tabs on the right side of the window, enter the appropriate property values. Use the Agent Tab to define the agent and designate the agent as a supervisor. Use the Skill Group Membership Tab to map the agent to any skill groups. (See the Configuration Manager online help for more information.)

Note An agent team can have only one primary supervisor. There is no upper limit to the number of secondary supervisors for a team. Refer to the online help for instructions on how to assign a primary supervisor.

Step 5 When finished, click **Save**.

Create agent teams

You can group individual agents into agent teams that supervisors can manage. Agent teams are assigned to specific peripherals, so you must assign all agents of a given team to the same peripheral. You assign agents individually to agent teams.

When configuring agent teams, be aware of the following rules:

- An agent can be a member of only one agent team.
- An agent team can have only one Primary Supervisor.
- A supervisor can be a supervisor of any number of agent teams.
- A supervisor for an agent team can also be a member of that agent team.
- All agents belonging to an agent team and all supervisors for that agent team must be on the same peripheral.

For more information on team limits, see the appendix on system requirements in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html.

Procedure

Step 1 From the Configuration Manager, select **Configure ICM** > **Peripherals** > **Agent Team** > **Agent Team List**.

Step 2 Click **Retrieve** and then **Add** to add a new agent team.

Step 3 Click the **Attributes** tab and enter values in the following fields:

Name. Enter an enterprise name for the agent team that is unique within the enterprise.

Peripheral: Enter the name of the agent team peripheral. You can select the name from the drop-down list.

Supervisor Script Dialed Number: Select a dialed number for the agent team from the drop-down list. If you have not created a supervisor script, select the default, “none”. When you create the script, return to this screen and enter the dialed number for the script.

Description: Enter additional information about the agent team.

Step 4 Click the **Members** tab and click **Add**.

Step 5 Choose the agents that you to assign to the team and click **OK**.

Step 6 Click the **Supervisor** tab and choose the supervisor from the Primary Supervisor drop-down list.

Step 7 To add a secondary supervisor, click the **Add** button and select a secondary supervisor from the list. Click **OK**.

Step 8 Click **Save** and then click **Close**.

Configure Network VRUs

Use the Configuration Manager tool to configure Network VRUs.

After you configure a Network VRU and VRU scripts, you can use the Script Editor to write a routing script to send a call to the VRU and invoke a specific VRU script.

See *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html for more information.

Create Network VRU Target

Procedure

Step 1 Within the Configuration Manager, select **Tools** > **Explorer Tools** > **Network VRU Explorer**.

The Network VRU Explorer window appears.

Step 2 In the Network VRU Explorer window, click **Retrieve** to enable **Add Network VRU** .

Step 3 Click **Add Network VRU**.

The Network VRU property tab appears.

Step 4 Complete the Network VRU property tab.

The Name and Type fields are required. All other fields are optional.

The ECC Payload field provides the name of the ECC payload that has scope for interactions with this network VRU. For additional information refer to the Online Help.

Step 5 Click **Save** to apply your changes.

Define Network VRU Label

You must associate all VRU Types (except Type 6) with a Network VRU label.

Procedure

Step 1 In the Network VRU Explorer window, click **Retrieve** and select the Network VRU you want to add the label to.

The Label property tab appears.

Step 2 Complete the Label property tab.

The **Routing client**, **Label**, and **Label type** fields are required. All other fields are optional. For additional information refer to the online Help.

Step 3 Click **Save** to apply your changes.

Set Default Network VRU and Range of Correlation Numbers

For Network VRUs, you must use the System Information dialog to define a range of correlation IDs so the system software can communicate with the VRU about the call.

Procedure

Step 1 Within the Configuration Manager, select **Tools** > **Miscellaneous Tools** > **System Information**.

The System Information window appears.

Step 2 In the System Information window, select the **Default Network VRU**.

Step 3 Enter the **Minimum Correlation Number**.

Step 4 Enter the **Maximum Correlation Number**.

For additional information refer to the online help.

Step 5 Click **Save** to apply your changes.

Configure scripts

Network VRU scripts

VRU scripts differ from routing scripts. A configured VRU script runs only when the Unified CCE instructs it to do so from a routing script. A VRU script on the Unified CCE is the configured record for the VRU script that resides on the VRU system. A VRU script runs to collect digits, play hold music, or perform many other common functions.

After you configure the VRU scripts, you can use the Script Editor to write a routing script to send a call to the VRU and invoke a specific VRU script.

For deployments that include the Unified CVP, use the Translation Route to VRU node to send calls to the Network VRU and invoke VRU scripts. Do not use Translation Route to VRU node for deployments that use the Unified CCE System PG. Instead, use any one of Queue to Skill Group or Send to VRU nodes.

Routing and administrative scripts

A *routing script* processes call routing requests from a routing client. Typically it examines several targets and applies selection rules to find an available qualified agent or a target with the shortest expected delay. You can set up different routing scripts to run for different types of tasks. You can define call types in terms of the telephone number the caller dialed, the number the caller is calling from, and additional digits entered by the caller. For each call type, you can schedule different routing scripts to run on different days or at different times of the day.

An *administrative script* runs periodically to perform a task, such as setting variables.

Configure Network VRU scripts

Procedure

Step 1 From the Configuration Manager, select **Tools > List Tools > Network VRU Script List**.

The Network VRU Script List dialog box opens.

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

Step 3 On the Attributes tab, enter the configuration information for the VRU script as follows:

Network VRU. Specify the Network VRU with which this script should be associated.

VRU Script Name. Enter script name; for example, BasicQ.

Name. Enter the script file name; for example, BasicQ.aef

Timeout [seconds]. Enter 180.

Configuration param. Leave blank.

Customer. Choose the same Unified CCE customer you chose for call type from the drop-down list.

Step 4 Check the **Interruptible** check box.

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

Troubleshoot Network VRU scripts

If a timeout occurs on a VRU script, it is possible that the Router does not notify the VRU PIM that a timeout has occurred. Because the VRU PIM is not informed of the problem, it does not notify the VRU to cancel the script.

At this point, the options for script flow include the following:

- The failure path in the Router script sends the call to a label, the VRU PIM gets a Connect and, if the VRU supports it, generates a Cancel message. This is the most common result.
- Before the Router picks a label, the VRU script completes and the VRU sends a Script Result message to the Router. The Router then sends a Dialogue Failure Event because it is not expecting a Script Result. This is the next most common result.
- The failure path in the Router script tries to run another VRU script. This is not a common result.

Currently, the best resolution to this problem is to use longer time-outs or create shorter VRU scripts. Be aware that the failure exit from the Run VRU Script node is a problem that you may need to resolve.

VRU error checking

A special call variable VruStatus, allows you to check the result of the last VRU node (Send To VRU/Translation Route to VRU/Run VRU Script) that the Unified CCE processed. The following table lists the values for this variable.

Value	Meaning	Description
0	VRU_SUCCESS	The last VRU node was successful.
1	VRU_ERROR	The last VRU node failed because of a routing or configuration error.
2	VRU_TIMEOUT	The last Send To VRU or Translation Route to VRU node failed because the routing client did not respond within 20 seconds or the last Run VRU Script node failed because the timeout limit defined for the script expired.
3	VRU_ABORTED	The last VRU node did not complete because the caller ended the call or was otherwise lost. (Because this causes the routing script to terminate immediately, this value is never seen.)
4	VRU_DIALOG_FAILED	The last VRU node failed because communication with the VRU ended unexpectedly.
5	VRU_SCRIPT_NOT_FOUND	The VRU failed because the referenced VRU script was not found in the Unified CCE configuration.

Configure routing and administrative scripts

After you complete your Unified CCE configuration, you can write routing scripts and administrative scripts. You create, maintain, and monitor these scripts using the Script Editor.

For Information about	See
Creating Unified CCE scripts	*Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html
Designing scripts for Unified CCE using the Script Editor	*Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html
Planning scripts for your Unified CCE reporting needs	*Cisco Unified Contact Center Enterprise Reporting User Guide* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html
Creating scripts for Outbound Option	*Outbound Option Guide for Unified Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps524/prod_installation_guides_list.html

Configure Agent Targeting Rules

The Agent Targeting Rules (ATR) configures call routing by specifying the agent extension range, instead of configuring Device Targets and Labels for every phone/Routing Client. This simplifies the call routing configuration for the Agent PGs. Also, this feature reduces the amount of memory used by the Router because a large number of Device Targets and Labels are replaced by a few rules. ATRs are therefore, the preferred method for installation.

Before you begin

You must configure the PGs and routing clients before you configure the Agent Targeting Rules.

Procedure

Step 1 From the Configuration Manager, choose one of the following:

- **Configure ICM** > **Targets** > **Device Target** > **Agent Targeting Rule**.
- **Tools** > **List Tools** > **Agent Targeting Rule**.

The ICM Agent Targeting Rules dialog box opens.

Step 2 Click **Retrieve**.

Step 3 Click **Add**.

Step 4 Enter a name for the rule.

Step 5 Select a peripheral where the rule will be associated.

Step 6 Select the rule type:

- Agent Extension
- Substitute Agent Extension: Enter the agent extension prefix and agent extension length.
- Translation Route: Select a Translation Route.

  For the Translation Route option, you must also configure the Translation Route DAIS as dialed numbers associated with the target agent's peripheral routing client in Unified CCE. You must map the dialed numbers to the route points that are configured in Unified Communications Manager and associated with the JTAPI user. This is necessary to complete the Translation Route Rule.

Step 7 Select one or more routing clients that can initiate the route request.

Step 8 Enter the agent's extension range.

Step 9 Click **Save**.

Step 10 Test the rule configuration by routing calls from each routing client to each agent extension you defined. If you defined a range, simplify the test by testing the lower and the upper limits of the agent extension, and a sampling of the extensions in between the range limits.

Configure translation routes

Use the Translation Route wizard to configure the translation routes for the Unified Communications Manager and VRU peripherals. This wizard automates the correct associations with peripheral targets, labels, and routes.

Note Run the Translation Route Wizard only if your Unified CCE solution uses Unified CVP.

Procedure

Step 1 In the Configuration Manager, select **Tools** > **Wizards** > **Translation Route Wizard**.

The Translation Route Wizard introductory dialog box opens.

Step 2 Click **Next**.

The Acquire Lock and Select Configuration Task dialog box opens.

Step 3 Select **Create New**.

Step 4 Click **Next**.

The Define Translation Route dialog box opens. The graphic on the left of the dialog box shows the entities you are defining while using the Translation Route Wizard.

Step 5 Enter a long and short name for the translation route and, optionally, a description (the short name is used in forming target names).

Step 6 Click **Next**.

The Select Configuration dialog box opens.

Step 7 Choose the single peripheral, single routing client configuration from the drop-down list.

The graphic changes to show the configuration you select.

Step 8 Click **Next**.

The Select Peripheral Gateway, Peripherals, and Services dialog box opens.

Step 9 Enter values for the following fields:

Peripheral Gateway. Choose the gateway target for the translation route.

Peripheral. Choose the single peripheral or the peripheral to route calls to.

Service/Service Array. If the translation route is associated with a single peripheral, choose the service associated with the translation route. If the translation route is associated with multiple VRUs, then select a service array.

Step 10 Click **Next**.

The Select Routing Clients and Dialed Numbers dialog box opens. Use this dialog box to specify the Unified Communications Manager peripheral (or VRU peripheral) as the routing client from which translation routed calls originate. For the Unified CCE the dialed number string is not applicable.

Step 11 Click **Next**.

The Select Network Trunk Groups for Routing Clients dialog box opens. Choose at least one network trunk group to be used in peripheral targets associated with the translation route.

Step 12 Choose a routing client, select a network trunk group value for it, and click **Add**.

The Network Trunk Group appears in the list at the bottom of the dialog box.

Step 13 Click **Next**.

The Configure DAIS dialog box opens.

Step 14 Use this dialog box to specify the DAIS values that map to route points on the VRU. Do one of the following:

- To enter a specific DAIS value, click **Add DAIS** and enter the value.
- To add a range of DAIS values, typically required by a translation route, click **Add DAIS Range**.

A dialog box prompts you to enter a starting and ending DAIS value. The Translation Route Wizard automatically generates the DAIS values in the range.

Step 15 Click **Next**.

The Configure Label dialog box appears.

Step 16 Use this dialog box to define a label that maps to the DAIS/CTI route points. A label consists of a prefix and a suffix. Each DAIS value requires a unique label. Do one of the following:

- Enter prefixes and suffixes individually.
- Use the buttons in this dialog box to set a range of values or to base the prefix or suffix values on the DAIS values.

Step 17 Click **Next**.

The Wizard Complete dialog box opens.

Step 18 Click **Create Translation Route** to create the translation route and its associated entities.

First, the Translation Route Wizard displays a success message and then the dialog box appears.

Step 19 Do one of the following:

- To see details about the translation route you just created, click **Run Report**.
- To return to the beginning of the Translation Route Wizard and perform a new task, select **Start New Task** and click **Finish**.
- To exit the Translation Route Wizard, click **Finish**.

Note You can also use the Translation Route Explorer to create a translation route or to modify a translation route that you created with the Translation Route Wizard. Select **Configuration Manager** > **Tools** > **Explorer Tools** > **Translation Route Explorer**.

Configure Skill Groups or Precision Routing

Skill groups are collections of agents that share a common set of skills. Skill groups are associated with a peripheral and are members of Services. You can associate agents with one or more skill groups.

To configure skill groups, you create skill groups, add the skill groups to services as members, and assign agents to one or more skill groups.

Precision routing offers an alternative to skill group routing. Using Unified CCE scripting, you can dynamically map the precision queues to direct a call to the agent who best matches the precise needs of the caller.

To configure precision routing, you create attributes, assign attributes to agents, create precision queues, and create routing scripts.

Configure Skill Groups

Add skill groups

You configure skill groups to group agents with similar skills. You can associate agents with one or more skill groups. Skill groups are associated with a specific Unified Communications Manager PIM. You can group skill groups from multiple PIMs into Enterprise Skill Groups. You can direct calls to (routed to) Enterprise Skill Groups to share the load across multiple call centers or Unified Communications Manager installations. You can do reporting on Enterprise Skill Groups.

Agents are assigned one or more skills by associating the agent with the desired skill group.

After you create services and skill groups, you associate one or more skill groups with a service by making them members of that service.

A default skill group is created automatically when you create system PGs. The default skill group acts as a bucket to capture information about calls not routed by Unified CCE. (A call placed directly to an agent extension is an example of such a scenario.) If you deploy multichannel applications in your Unified CCE system, default skill groups are created for each Media Routing Domain that you configure.

Note An agent must be assigned to at least one skill group to log in.

Procedure

Step 1 From the Configuration Manager, select **Configure ICM** > **Peripherals** > **Skill Group** > **Skill Group Explorer**.
The Skill Group Explorer dialog box opens.

Step 2 In the Select filter data section, select the peripheral from the drop-down list:

Step 3 Click **Retrieve** and then click **Add Skill group** to add a new skill group for the selected peripheral.

Step 4 Click the **Skill Group** tab and enter values for the following:

Media Routing Domain. Use Cisco_Voice for agents that do not use other media. For more information, see the *Enterprise Chat and Email Installation Guide (for Unified Contact Center Enterprise)* at https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html.

Peripheral Number. Enter the skill group number as known by the peripheral. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.

Peripheral Name. Enter the local name for the skill group. This value must be unique among all skill groups for the peripheral, but does not need to be unique across peripherals.

Name. The Configuration Manager generates the value for this field. This value is a unique name for the skill group made up of a default value from the peripheral enterprise name and the skill group peripheral name.

Available Holdoff Delay. For the Unified CCE peripheral type, set this field to 0.

Priority. This field is read-only and defaults to 0.

Extension. Leave blank for the Unified CCE peripheral type.

ICM picks the agent. Check this check box.

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

Step 6 Repeat this procedure for any additional skill groups.

Assign skill groups as service members

To make a skill group a member of a service, you establish mappings of skill groups to services. Each skill group can be mapped to zero, one, or more services. Each service can have zero, one, or more skill group members.

Procedure

Step 1 From the Configuration Manager, choose **Configure ICM** > **Peripherals** > **Service** > **Service Explorer**. The Service Explorer dialog box opens.

Step 2 Click **Retrieve**.

Step 3 Click the service that directs the skill group and then click the **Service Members** tab.

Step 4 On the Service Members tab, click **Add** to associate a skill group with the service.

Step 5 Click **OK**.

Step 6 Click **Save** and then click **Close**.

Step 7 Repeat this procedure for each skill group you want to associate with a service.

Assign agents to skill groups

Agents must be assigned to at least one skill group in order to log in. You can assign agents to the most appropriate skill groups according to their talents and skills to ensure that the most appropriate agent for a request responds to the customer.

Procedure

Step 1 From the Agent Explorer dialog box, choose the **Skill Group Membership** tab.

Step 2 From the Skill group name list, select the skill groups to which you want this agent assigned.

Step 3 Click **Add**.
The Add Skill Group Membership box opens, showing the skill groups to which the agent has been assigned.

Step 4 Click **OK**.

Step 5 Click **Save** and then click **Close** on the Agent Explorer dialog box.

Step 6 Repeat this procedure to assign additional agents to skill groups.

Note You can remove agents from the Skill Group tab if necessary by selecting the agent and clicking **Remove**, then **Save**.

Configure Precision Routing

To configure precision routing, use the Unified CCE Web Administration application, which links to various precision routing gadgets. To access the application, click the **CCE Web Administration** shortcut on your desktop, or copy the following URL into your browser: **https://distributor ip/cceadmin**.

For more information on precision routing, 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

Add Attributes

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Attributes**.

Step 2 In the **List of Attributes** window, click **New**. The **New Attributes** window has two tabs: General and Member.

Step 3 Complete the following fields on the **General** tab:

Field	Required	Description
Name	yes	Type a unique attribute name. For example, to create an attribute for mortgage insurance, type *mortgage*.
Description	no	Enter a maximum of 255 characters to describe the attribute.
Type	no	Select the type: Boolean or Proficiency.
Default	no	Select the default (True or False for Boolean, or a number from 1 to 10 for Proficiency).

Step 4 Click **Save**.

Search for Agents

The Search field in the Agents tool offers an advanced and flexible search.

Click the + icon at the far right of the **Search** field to open a popup window, where you can:

- Select to search for agents only, supervisors only, or both.
- Select to search for all agents or only ECE enabled agents.
- Enter a username, agent ID, first or last name, or description to search for that string.
- Enter one or more site names separated by spaces. (Site is an OR search.)

- Enter one or more peripheral set names separated by spaces (Peripheral Set is an OR search). The search is case-insensitive and does not support partial matches.

Note Search by department is available only when departments are configured.

Assign Attributes to Agents

Procedure

Step 1 With the selected agent displayed, click the **Attributes** tab.

Step 2 Complete the **Attributes** tab:

This tab shows the attributes associated with this agent and their current values.

Click **Add** to open a popup list of all attributes, showing the name and current default value for each.

a) Click the attributes you want to add for this agent.
b) Set the attribute value as appropriate for this agent.

Add Precision Queue

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Precision Queues**.

This opens a **List of Precision Queues** window showing all precision queues that are currently configured.

Step 2 Click **New** to open the **New Precision Queue** window. Complete the fields.

Name	Required	Description
Description	no	Enter up to 255 characters to describe the precision queue.
Media Routing Domain	no	MRDs organize how requests for media are routed. The system routes calls to skill groups or precision queues that are associated with a particular communication medium; for example, voice or email. This field defaults to *Cisco_Voice*.

Name	Required	Description
Service Level Type	yes	Select the service level type used for reporting on your service level agreement. Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation. • **Ignore Abandoned Calls** (the default): Select this option if you want to exclude abandoned calls from the service level calculation. • **Abandoned Calls have Negative Impact:** Select this option if you want only those calls that are answered within the service level threshold time to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level threshold time. • **Abandoned Calls have Positive Impact:** Select this option if you consider a call that is abandoned within the service level threshold time as a treated call. With this configuration, abandoned calls have a positive impact on the service level.
Service Level Threshold	yes	Enter the time in seconds that calls are to be answered based on your service level agreement, from 0 to 2,147,483,647. The time that you enter in this field is used to report on service level agreements and does not affect how long a call remains in a precision queue. The length of time a call remains in a step is determined by the wait time for each individual step.

Name	Required	Description
Agent Order	yes	Select an option to determine which agents receive calls from this queue. The ordering of agents does not dictate the agents who are selected into a Precision Queue step. Agents are included or excluded based on the conditions specified for the step. • **Longest Available Agent** (the default): The default method of agent ordering for a precision queue. The call is delivered to the agent who has been in the available (or ready) state the longest. • **Most Skilled Agent:** The call is delivered to the agent who has the highest competency sum from all the attributes pertinent to the Precision Queue step. In an agent-rich environment, this can mean that more competent agents would be utilized more than less competent agents. • **Least Skilled Agent:** The call is delivered to the agent who has the lowest competency sum from all the attributes pertinent to the Precision Queue step.
Bucket Intervals	no	Select the bucket interval whose bounds are to be used to measure the time slot in which calls are answered. The field defaults to the system default. To select a different bucket interval:

Step 3 Click the numbered Step Builder link (Step 1, Step 2, and so on) to build a precision queue step in the **Step Builder** popup window.

Step 4 When you have finished adding, click **Save**.

Consider If Formula for Precision Queue

If you are not on the last step of the precision queue, then you can enter a *Consider If* formula for that step. A Consider If formula evaluates a call (within a step) against additional criteria. Each time a call reaches a step with a Consider If expression, the expression is evaluated. If the value for the expression returns as true, the call is considered for the step. If the value returns as false, the call moves to the next step. If no expression is provided for a step, the step is always considered for calls.

To add a Consider If formula, type the formula into the **Consider If** box. Alternatively, you can use the Script Editor to build the formula and then copy and paste it into the **Consider If** box. Objects used in Consider If formulas are case-sensitive. All Consider If formulas that you add to a precision queue must be valid. If you add an invalid formula, you cannot save the precision queue. To ensure that the formula is valid, use Script Editor to build and validate the formula.

Only the following scripting objects are valid in a Consider If formula:

- Call
- PQ
- Skillgroup
- ECC
- PQ Step
- Call Type
- Custom Functions (You can create custom functions in Script Editor.)

It is possible that a valid Consider If formula can become invalid. For example, if you delete an object used in the formula after you create or update the precision queue, the formula is no longer valid.

Consider If Formula Examples

- **PQ.PQ1.LoggedOn > 1**--Evaluates whether there is more than one agent logged in to this queue.
- **CallType.CallType1.CallsRoutedToday > 100**--Evaluates whether more than 100 calls of this call type were routed today.
- **PQStep.PQ1.1.RouterAgentsLoggedIn > 1**--Evaluates whether there is more than one router agent logged in to this queue for Step 1.
- **CustomFunction(Call.PeripheralVariable1) > 10**--Evaluates whether this formula using a custom function returns a value greater than 10.

Build Precision Queue Steps

Every precision queue must have a step, and every step must have an Expression. An Expression is a collection of attribute terms.

Procedure

Step 1 Click the numbered step link in the **Steps** panel (Step 1, Step 2, and so on).

The step number popup window opens.

Step 2 Build the first step as follows.

a) Click the **magnifying glass** icon to the right of the Select Attribute field in the Expression 1 panel.
b) Select an attribute from the list.
c) Use the two **Select** fields to establish the terms of the attribute. Click the first **Select** field to choose an operator.

- For Boolean attributes, choices are the operators for Equal and Not Equal.
- For Proficiency attributes, choices are the operators for True, False, Less Than, Less Than or Equal To, Greater Than, and Greater Than or Equal To.

d) Click the second **Select** field to choose a value.

- For Boolean attributes, values are True and False.
- For Proficiency attributes, values are numbers from 1 to 10.

Your selection creates an attribute term for the Expression.

Step 3 To add a second attribute to the first Expression, click **Add Attribute** in the **Expression 1** row.

a) Select **AND** or **OR** to establish the relationship between the first and second attributes.
b) Repeat steps 2b, 2c, and 2d.

Step 4 Continue to add attributes to Expression 1.

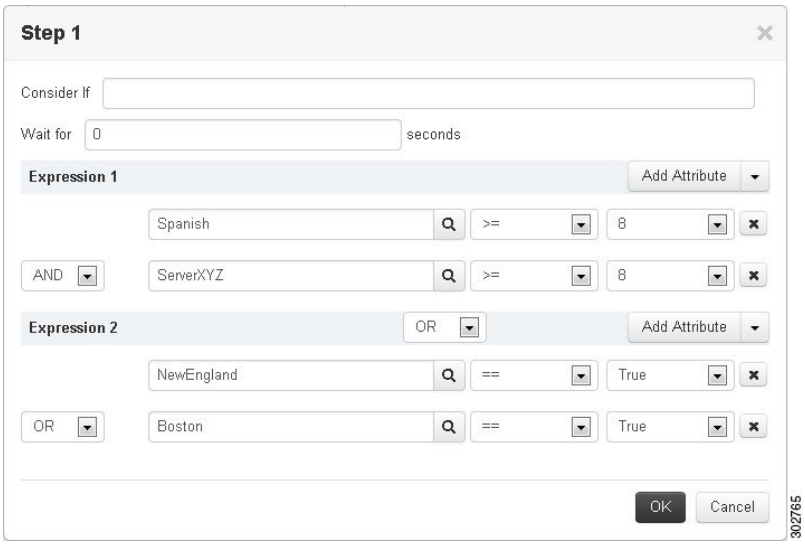
All attributes within an expression must be joined by the same logical operator. They must all be ANDs, or they must all be ORs.

Step 5 To add a second Expression, click the **Add Attribute** drop-down in the **Expression 1** row and select **Add Expression**.

Step 6 Select **AND** or **OR** to establish the relationship between the first and second Expressions.

Step 7 Add attributes to Expression 2.

Step 8 Continue to add Expressions as needed.



In this example, a Spanish caller located in the Boston area needs an onsite visit from a technician to repair his ServerXYZ. An ideal agent should be fluent in Spanish and have the highest proficiency in ServerXYZ.

This can be seen in Expression 1. Expression 2 allows us to specify that the selected agent must also be from either Boston or the New England area.

Step 9 When you have completed the step, click **OK** to add it to the precision queue.

Step 10 To build the next step, click **Add Step**.

Each successive step is prepopulated with the Expressions and attributes of its predecessor. Decrease the attribute qualifications and competencies in successive steps to lower the bar such that the pool of acceptable agents increases.

Step 11 When you have created all steps, you can open any step *except the last* and enter values in the **Consider if** and **Wait for** fields.

- **Consider if** is a formula that evaluates a call within a step against additional criteria. (See Consider If Formula for Precision Queue, on page 35 for more information about Consider If.)
- **Wait for** is a value in seconds to wait for an available agent. A call will queue at a particular step and wait for an available agent matching that step criteria until the number of seconds specified. A blank wait time indicates that the call will proceed immediately to the next step if no available agents match the step criteria. Wait time defaults to 0 and can take a value up to 2147483647.

Configure routes

The *route* is a value returned by a routing script that maps to a target or a peripheral. Those targets include services, skill groups, agents, translation routes, queue points, or CTI route points. The Unified CCE converts a route to a device target to direct to the request destination.

When you create a route, you associate the route with a service.

Procedure

Step 1 From the Configuration manager, choose **Tools** > **Explorer Tools** > **Skill Group Explorer**.
The Skill Group Explorer dialog box opens.

Step 2 Click **Retrieve**.

Step 3 Choose the skill group for which you are creating the route.

Step 4 Click **Add Route**.

The Route tab opens.

Step 5 In the Route tab, enter information in the following fields:

Skill group priority. The value 0 indicates a base skill group. This is the default when there is only one skill group and there are no priorities.

Name. The enterprise name of the route.

Description. Enter an optional description of the route.

Service Name: The name for the service.

Step 6 Click **Save**.

Caution When you break the association between a route and a peripheral, the Unified CCE removes the Route ID value from all peripheral targets that reference that route.

Perform Bulk Configuration

Access Bulk Configuration Tools

Procedure

Step 1 Double-click **Configuration Manager** in the Administration Data Server group or the Administration Client group.

Step 2 In the Menu selection box, select **Tools** > **Bulk Configuration**.

Step 3 From the submenu selection list, select **Insert** if you need to insert data or **Edit** if you need to edit.

Step 4 In the next menu selection list, select the type of table with which you need to work.

Add New Records

You can add records by inserting multiple blank rows (records) and filling in the data or by importing the data.

You can also edit the data you insert when you insert it.

Insert New Records

To insert a new record:

Procedure

Step 1 In the **Bulk Configuration** > **Insert** menu, select the name of the data table to which you want to add records. The appropriate Insert window opens, automatically displaying one new row.

Step 2 To create additional rows, enter the number of additional rows in the Quantity field and click **Insert**. The additional rows are added in the Insert window.

Step 3 Enter the data in the rows:

a) If you want to edit individual fields in the new rows, type the information you want in each of the fields and skip to Step 8.

b) If you want to edit a column in multiple rows so that a range of values is entered, continue to Step 4.

Note For other ways of entering data into multiple rows, see Edit Range of Data, on page 41

Step 4 Select the rows in the column you want to modify.

Step 5 Click **Edit Range**. The Edit Range dialog appears.

Step 6 Enter a prefix (optional), the start value for the range, and a suffix (optional). The generated values are listed in the dialog.

Step 7 Click **OK** to close the Edit Range dialog and apply the values to the column you selected.

Step 8 When you have finished setting fields in the new rows, press **Enter** to apply your changes to the Unified CCE database.

Note You can leave empty rows, the system ignores them. No changes are made to the database until you press **Enter**.

Import Data

You can import data from a specified text file into the opened database table. You can import whole records or only columns of data if the data matches (see Step 3 of the following procedure). The process cancels if any error occurs during the import process.

Procedure

Step 1 In the Insert or Edit window, click **Import**.

Step 2 In the Import dialog, click **File**.

Step 3 In the File Open dialog, select the file containing the data that you want to import and click **Open**.

The Import File Data area displays the first few lines of the opened file.

- When importing data in the Edit mode, the following rules apply:
  - The Bulk Configuration tool reads only those records whose primary key values match those of records in the Edit window.

    If a record does not match the primary key value, the record is considered to be an error and a message box with the primary key value pops up to ask you to correct the problem.
  - If any field in the import record is null, the corresponding field value in the grid window become blank for an edit cell or uses the default value for a drop-down list cell.
  - If any field is missing in the import file, the corresponding field in the Edit window remains unchanged.
  - If there is a larger number of records in the file to be imported than the number of rows in the grid, it is considered an error and a message box pops up asking you to correct it.
  - If there is a duplicated primary key in the file to be imported, it is considered an error and a message box with the duplicated primary key value pops up asking you to correct it.
  - After importing, all records imported (including records marked for deletion in the grid) are marked as “Changed” regardless of whether the value is changed or not.
  - After importing, the records display in index order (ordered by logical keys). If you did not sort before importing, the order appears the same after the import.
- When importing data in the Insert mode, the following rules apply:
  - Only a single import is supported and any existing rows are removed from the grid. When you click **Import**, the following message box pops up if there is any record in the grid:

```
All the existing data will be replaced by the data to be imported.
If you want to retain the current data on the grid please click
the Cancel button then save or export the existing data. Click the
OK button to proceed with the importing.
```

- After importing, all rows are marked as “New” and the ordering is the same as that in the file imported from.
- In the Import Insert mode, the tool reads only those records whose primary key values are not presented. If the primary key field is selected for file to be imported, it is considered an error and a message box with the primary key field name pops up asking you to correct the problem.
- If any field in the import record is null, the corresponding field value in the grid window becomes blank for an edit cell or uses the default value for a drop-down list cell.

Note If headers are included in the imported file, the **Add** and **Remove** buttons are not enabled and you can only import the records as a whole. In that case, skip to Step 6.

Step 4 If the imported data does not contain headers, in the Available Fields list box, select the names of the fields to import that match the data and click **Add**.

Step 5 To change the order of the columns, select a column and move it within the list by clicking **Up** or **Down**.

Step 6 Click **OK**. The data is imported into the data table.

Data File Format

The import and export files used by the Bulk Configuration tool can optionally include a header that identifies the table and columns in the file. The header is followed by one line for each row of data.

The following rules apply to file headers:

- A line beginning with a number sign (#) is a comment and is ignored.
- Blank lines are also ignored.
- The header content is indicated by a line beginning with two underline characters and the word **TABLE** or **COLUMNS**. The following line contains the name of the table or the name of the columns. For example:

```
__TABLE

Call_Type __

COLUMNS

CallTypeID EnterpriseName Description Deleted CustomerDefinitionID
```

- All column names must be on a single line and are separated by Tab characters.

  The following rules apply to the data in the files:

  - One row of table data per line.
  - Column values must be in the same order in all rows. If columns are specified in the header, the columns in the data rows must be in the same order.
  - Column values are separated by a single Tab character.

- Fields intentionally left blank must be represented by two adjacent Tab characters or a Tab character at the end of a line. On import, the default value is used for such a value.
- String values may include spaces.
- An error occurs on import if a line contains too few or too many values.

Note A simple way to create the import file with a valid format is to use Excel and save the file as Text (Tab delimited) (*.TXT).

Select Data

You can select whole records for importing, exporting, setting security, deleting, or undeleting. Or, you can select the same field in multiple records for simultaneous editing.

Select Records

Click in the left-most numbered field in a row to select that row and highlight it. Click in any other field in a row to select the row but not highlight it.

Select One Field in Multiple Records

You can select one edit-control field (when there is no section box in the field) in multiple records in any of the following three ways:

- Click the field where you want to start and, keeping the left mouse button held down, move the cursor to the last field.
- Click the field where you want to start. While holding down the **Shift** key, click the last field.
- Click the field where you want to start. While holding down the **Shift** key, click the down arrow to select.
- Press **Ctrl,** then click on each field you wish to select. This allows you to select a discontinuous group of fields.

Edit Range of Data

You can edit a range of data in a table column in three ways:

Procedure

- Apply a single value to a range of edit-control fields
- Apply a single value to a range of selection-box fields
- Apply a range of values to a range of fields

Apply a Single Value to a Range of Edit-Control Fields

An *edit-control field* is one you can edit that does not contain a selection box.

To apply a single value to a range of edit-control fields:

Procedure

Step 1 Make your selection: click the field where you want the range to start and, keeping the left mouse button held down, move the cursor to the last field in the range.

Step 2 Type the new entry that you want to appear in all the fields.

Step 3 Click **Enter** or **Tab**. This applies the change to all the records in the range and moves the focus to the next data field.

Apply a Single Value to a Range of Selection-Box Fields

To apply a single value to a range of selection-box fields:

Procedure

Step 1 Select the first field where you want the range to start.

Step 2 Press the **Shift** key and hold it down for steps 3, 4, and 5.

Step 3 Click the selection-box down arrow but keep the left mouse button held down and select the fields you want in the range.

Step 4 Click the last field in the selection to display the selection list. You can also open the selection box by pressing **Alt** + an arrow key.

Step 5 Click your selection.

Step 6 Click **Enter** or **Tab** (or any other field). This applies the change to all the records and moves the focus to the next data field.

Apply a Range of Values to a Range of Fields in a Column

To apply a range of values to a range of fields in a column:

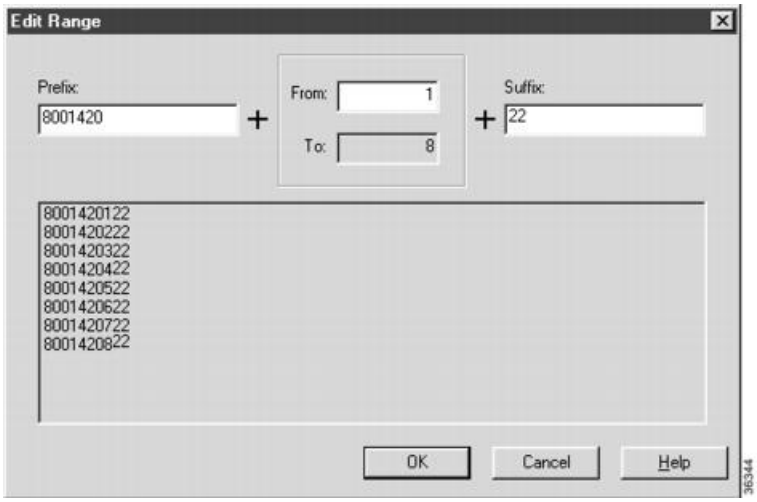
Procedure

Step 1 Select the range of fields in a database column. This enables the **Edit Range** button.

Note The **Edit Range** button does not work for selection-box fields.

Step 2 Click **Edit Range**. The Edit Range dialog displays.

Figure 1: Edit Range Dialog Box



Step 3 In the Edit Range From field, enter the first number of the range.

Step 4 In the Prefix and Suffix fields, you can optionally enter substrings to appear before or after each value. The Edit Range dialog lists the generated values.

Note When entering a numeric range, you may also enter leading zeros to ensure proper alignment (that is, 001 to 999).

Step 5 Click **OK**. This applies the changes to the fields you selected in the Insert or Edit window.

Configure Cisco Unified Intelligence Center

Sign In to Administration Console

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

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

Procedure

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

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

Configure SQL User Account

Procedure

Step 1 Launch Microsoft SQL Server Management Studio using System Administrator login credentials on the Administration and Data Server.

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

Use these steps to create login accounts for the **Cisco Unified Intelligence Center** reporting data sources and for Finesse connectivity to the AW Database on the **Cisco Finesse Administration** page.

Step 3 On the General Screen:

a) Enter the Login Name.
b) Select **SQL Server authentication**.
c) Enter and confirm the password.
d) Uncheck **Enforce password policy**.

Step 4 In the Server Roles page, check the **public** check box.

Step 5 On the User Mapping page, do the following:

a. Check the **Real-time database** and **Historical database** check boxes.

b. In the **Users mapped to this login** area, check the **master** check box. This is required only for an SQL user configured to work with Live Data.

c. In the **Database role membership for** area, do the following:

- For CUIC and Finesse users, check the **db_datareader** and check box.
- For Live Data users, check the following check boxes:
  - **db_datareader**
  - **db_datawriter**

Note The database role **public** is checked by default. This role is required for CUIC, Finesse, and Live Data users.

Step 6 Click **OK**.

What to do next

Note Ensure that you configure SQL User Account on both the primary and secondary AW databases.

Configure Data Sources

To integrate Unified Intelligence Center with Unified CCE, you must configure the following two data sources:

- Unified CCE Historical data source—This data source is added by default to support the Unified CCE stock historical reports and Unified CCE User Integration. Complete the Database Host, Database Name, and the Database User ID and Password fields for this data source and ensure that it is online before Unified CCE User Synchronization can occur.
- Unified CCE Realtime data source—This data source is added by default to support the Unified CCE stock real time reports. Complete the Database Host, Database Name, and the Database User ID and Password fields for this data source.

Depending on your environment, the Unified CCE Historical and Realtime data sources can point to the same machine.

You can run a CLI command to point each node to a unique IP Address for the Unified CCE Historical or Realtime data source. The command is `set cuic properties host-to-ip`. For more information about the CLI, see the *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

To integrate Unified Intelligence Center with Unified CVP, you must add a Unified CVP data source.

A Unified Intelligence Center data source is also installed by default. This data source represents the Unified Intelligence Center database on the node that stores records for reports, dashboards, and users maintained on that node. This data is replicated across all nodes in the cluster. You can edit the description for this data source, but *do not change other fields*. The Unified Intelligence Center data source for each node is configured by default to point to that member.

Configure Unified CCE Data Sources

Procedure

Step 1 From the Unified Intelligence Center Reporting application, click **Data Sources** drawer on the left panel to open the **Data Sources** page.

Step 2 Select the Unified CCE Historical Data Source.

Step 3 Click **Edit** to open the **Data Source Create/Edit** page.

Step 4 Complete the fields for the selected data source. See online help for guidance.

Note The name of the database instance is a required field only for Informix databases.

Step 5 Test the data source connection. Troubleshoot, if required.

Step 6 Save the data source.

Step 7 Repeat steps 2 through 6 for the Unified CCE Realtime data source.

Create Data Source for Cisco Unified CVP Report Data

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.
Port	Enter the port number. Typically, the port is 1526.
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 who is configured in the Operations Console 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.

Field	Value
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.

Cisco Unified Intelligence Center Reporting User Roles

There are seven User Roles, and a user can be assigned to one, any, or all of them. The roles are:

- Login User
- System Configuration Administrator
- Security Administrator
- Dashboard Designer
- Value List Collection Designer
- Report Designer
- Report Definition Designer

Depending on the size, staff, geographical distribution, and security practices of your call center, you might want to assign multiple user roles to a few people or to distribute user roles to many people.

Login User

By default, everyone who can sign in to Unified Intelligence Center is a Login User. Login Users have that role and only that role until the Security Administrator assigns additional roles or deactivates (removes) the Login User role.

A Security Administrator or System Application user can remove the login role from any user.

An active login user can:

- Log in to Unified Intelligence Center
- Open the Security drawer, access the User List, and edit his own User Information page; for example, to change his alias or phone number.

System Configuration Administrator

This user has all the rights of an active Login User and also:

- Has full access to the Data Sources drawer and its functions.
- Has full access to the Scheduler drawer and its functions.

Security Administrator

This user has all the rights of an active Login User and also has full access to the Security drawer and its functions.

Dashboard Designer

This user has all the rights of an active Login User and also has full access to the Dashboard drawer.

Value List Collection Designer

This user has all the rights of an active Login User and also:

- Has full access to the Value Lists drawer.
- Has View (Read) access to the Data Sources drawer.

Report Designer

This user has all the rights of an active Login User and also:

- Has full access to the Reports drawer.
- Has View (Read) access to the Data Sources and Value Lists drawers.
- Can access the Scheduler drawer to work with the user's own reports.

Report Definition Designer

This user has all the rights of an active Login User and also:

- Has full access to the Report Definition drawer.
- Has View (Read) access to the Data Sources and Value Lists drawers.

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.

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

Additionally, sample custom report templates are available from the Cisco Developer Network (https://developer.cisco.com/web/ccr/documentation).

Import Report Bundles

Procedure

Step 1 Sign in to Unified Intelligence Center at https://<hostname/ IP address of CUIC Publisher>:8444/cuicui, and click **Reports** in the left pane.

Step 2 Click **Import Report**.

Step 3 In the **File Name (XML or ZIP file)** field, click **Browse**.

Step 4 Browse to and select the report bundle zip file, and click **Open**.

Select a report bundle for the version of software deployed in the contact center.

Step 5 Select the location where you want to save the file.

Step 6 Click **Import**.

Step 7 Choose one:

- If the report or reports do not yet exist, you must provide the data source. From the **Data Source for ValueList** drop-down list, select the data source used. Then click **Import**.

  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 LiveData reports, the Data Source for ReportDefinition is LiveData Streaming and the Data Source for ValueList is UCCE Realtime. For real time reports, the Data Source is UCCE Realtime. For historical reports, the Data Source is UCCE Historical.

- If the report or reports do exist, a message appears asking you if you want to replace the existing report (which overwrites any report definition changes associated to it). Click **Yes**, **Yes to All**, **No**, or **No to All**.

Configure Unified Intelligence Center Administration

Complete the following procedure to configure Unified Intelligence Center Administration.

Procedure

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

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

a) For Host Address for the Primary Active Directory Server, enter the IP address of the domain controller.

b) For Port, enter the port number for the domain controller.

c) Complete the **Manager Distinguished Name** fields that are required for the customer.
d) Enter and confirm the password with which the Manager accesses the domain controller.
e) For User Search Base, specify users and the domain name and any sub-domain names .
f) For Attribute for User ID, select the required option.

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

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

Note For more details, see the online help.

Step 3 Configure syslog for all devices.

a) Choose **Device Management** > **Logs and Traces Settings**.
b) For each host address:
   - Select the associated servers and click the arrow to expand.
   - Select the server name.
   - In the **Edit Serviceability Settings** screen **Syslog Settings** pane, configure the Primary and Backup Host. Click **Save**.

Step 4 Configure SNMP for all devices, if used.

a) Select **Network Management** > **SNMP**.
b) Navigate to SNMP and for each server add the following:
   - V1/V2c Community Strings.
   - Notification Destination.

Configure Cisco Unified Customer Voice Portal

Configure Unified CVP Server

Set Up FTP Server

Procedure

Step 1 Install the FTP Service on the server.

a) Choose **Start** > **Administrative Tools** > **Server Manager**.

b) Expand **Roles** in the left panel of the Server Manager window.
c) Right-click **Web Server (IIS)** and click **Add Role Services**.
d) Check the **FTP Server** check box, click **Next** and then click **Install**, installation takes a few moments.
e) When the installation is complete, click **Close**.

Step 2 Enable the FTP Service on the server.

a) Choose **Start** > **Administrative Tools** > **Server Manager**.
b) Expand **Roles** in the left panel of the Server Manager window.
c) Expand **Web Server (IIS)** and then click **Internet Information Services (IIS) Manager**.
d) Expand hostname.
e) Right-click **Sites** and click **Add FTP Site**.
f) Enter a **FTP site name**.
g) Enter **c:\Inetpub\wwwroot** in the **Physical path** of the FTP site name, and click **Next**.
h) Enter the IP address of the CVP Server.
i) Select **No SSL** in SSL Options and then click **Next**.
j) Check the **Anonymous** and **Basic** check boxes.
k) Select **All Users** from the Allow Access To drop-down list.
l) Check the **Read** and **Write** check boxes, and then click **Finish**.

Step 3 Set the Basic Setting for the FTP Server.

a) Click **Sites** and then click the FTP server that you have created.
b) Click **Basic Settings** in the Actions tab and click **Connect as**.
c) Select **Application user (pass-through authentication)** option and click **OK** twice.

Configure Unified CVP Reporting Server

Create Reporting Users

Who can create a user:

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

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

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

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

Create Superusers

Procedure

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

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

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

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

Step 4 Click **Save**.

Set Up Active Directory Server for LDAP Users

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

Procedure

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

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

Step 3 Click **Test Connection**.

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

Sign In to Cisco Unified Intelligence Center Reporting Interface

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

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

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

Procedure

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

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

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

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

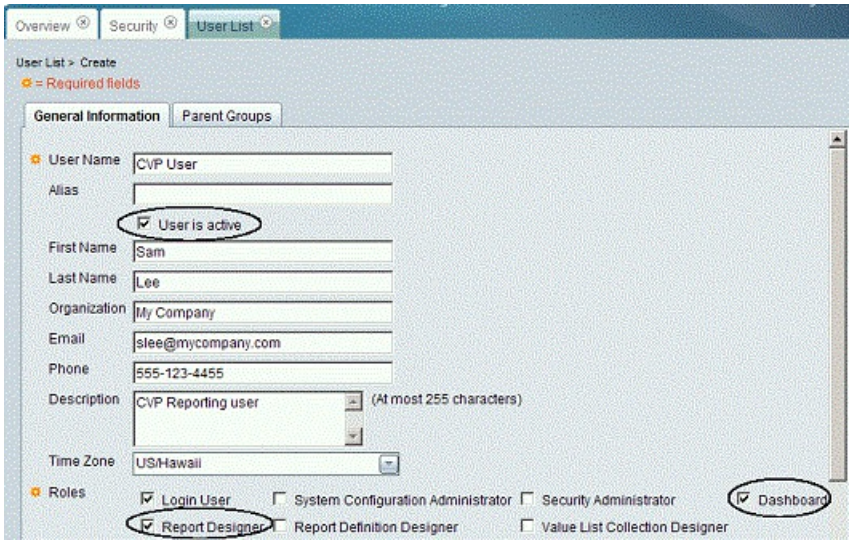
Step 5

Cisco Unified Customer Voice Protocol Reporting User Role Additions

Once Unified CVP users log in to Unified Intelligence Center, they are added to the Unified Intelligence Center database and appear on the user list.

New users are initially defined as Login Users: the lowest level user role of Unified Intelligence Center. A Unified Intelligence Center Security Admin user must access the User List page to check a **User is Active** check box and to grant additional user roles to the user.

Figure 2: User List Page



Obtain and Import Report Templates

Obtain Cisco Unified CVP Report Templates

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

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

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

Procedure

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

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

Import Unified CVP Report Templates

Procedure

Step 1 Launch the Unified Intelligence Center web application using the `URL https://<CUCI ADDRESS:8444/cuicui/`.

Step 2 Enter CUIC Username and Password.

Step 3 Create a folder to import the reports.

a) Click **Reports**.
b) From the toolbar, click **New** > **Folder**.
c) Enter the folder name and click **Save**.

Step 4 Import the report templates.

a) Click **Reports** > **New > Import**. You will be redirected to the CUIC legacy interface.
b) Click **Reports** > **Import Report**.
c) In the **File Name (XML or ZIP File)** field, click **Browse** and select the template file to import.
d) In the **Save To** field, expand the Reports tree and select the folder created to import the report template.
e) Click **Import**. CUIC validates the Report Definition ID in the template and successfully imports the template.

Note When one or more underlying Report Definitions do not exist in CUIC, you will be prompted to select a data source for the Report Definition and Value Lists. For information on creating Data Sources and Value Lists, see Cisco Unified Intelligence Center Report Customization Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html.

Configure Unified CVP Operations Console

Enable Unified CVP Operations Console

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

Procedure

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

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

Step 3 Go to **Start > All Programs > Cisco Unified Customer Voice Portal > Operation Console** to open the Unified CVP OPSConsole page.

Configure Unified CVP Call Server Component

Note

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

Procedure

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

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

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

Step 4 Click **Add New**.

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

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

Step 7 Click the **SIP** tab:

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

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

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

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

Example:

Prime server

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

Step 10 Click **Save & Deploy**.

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

Configure Unified CVP VXML Server Component

Procedure

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

Step 2 Click **Add New**.

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

Step 4 Configure the primary and backup CVP Call Servers.

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

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

Step 7 Click **Save & Deploy**.

Step 8 Repeat this procedure for all CVP Servers.

Configure Unified CVP Media Server

Procedure

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

Step 2 Click **Add New**.

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

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

Step 4 Click **Save**.

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

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

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

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

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

Step 10 Click **Deploy**.

Install Unified CVP Licenses

For instructions on installing Unified CVP licences, see the *Smart Licensing* section in *Administration Guide for Cisco Unified Customer Voice Portal* guide at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html.

Configure Gateways

Procedure

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

Step 2 Click **Add New**.

Step 3 On the General tab, configure as follows:

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

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

Step 5 Click **Save**.

Step 6 Repeat for every gateway.

Add Unified CCE Devices

Procedure

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

Step 2 Choose **Device Management** > **Unified ICM**.

Step 3 Click **Add New**.

Step 4 On the General tab, configure as follows:

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

Step 5 Click **Save**.

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

Add Unified Communications Manager Devices

Procedure

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

Step 2 Choose **Device Management** > **Unified CM**.

Step 3 Click **Add New**.

Step 4 On the General tab, configure as follows:

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

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

Step 5 Click **Save**.

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

Add Unified Intelligence Center Devices

Procedure

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

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

Step 3 Click **Add New**.

Step 4 On the General tab, configure as follows:

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

Step 5 Click **Save**.

Transfer Scripts and Media Files

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

Procedure

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

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

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

Step 4 Click **Default Gateway files**.

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

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

Configure SNMP

For more information about SNMP in Unified CCE, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html and *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_installation_and_configuration_guides_list.html.

Procedure

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

Step 2 Click **Add New**.

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

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

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

Configure SIP Server Group

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

Procedure

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

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

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

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

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

The FQDN should match the FQDN configured in the Enterprise Cluster FQDN setting on the Cisco Unified Communications Manager. For example, *cucm.cisco.com*. Adding the cluster subscriber nodes will load balance across all sub nodes.

Step 3 Create a server group for the gateway devices:

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

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

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

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

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

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

Configure Dialed Number Patterns

Dialed number patterns are required for:

- Agent Device
- Network VRU
- Ringtone
- Error

Procedure

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

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

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

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

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

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

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

Configure Cisco IOS Enterprise Voice Gateway

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

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

Procedure

Step 1 Configure the network interfaces:

```
interface GigabitEthernet0/0
 ip route-cache same-interface
 duplex auto
 speed auto
 no keepalive
 no cdp enable
```

Step 2 Configure global settings:

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

Step 3 Configure voice codec preference:

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

Step 4 Configure Unified CVP services and settings:

```
# Default CVP Services
application
 service new-call flash:bootstrap.vxml
 service survivability flash:survivability.tcl
 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

# Default CVP http, ivr, rtsp, mrcp and vxml settings
```

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

Step 5 Configure primary and secondary media servers:

```
#Configure the media servers where
# the primary matches the default media server defined in OAMP.
# the secondary is located on the opposite side of the primary.
ip host mediaserver ###.###.###.### # IP Address for primary media server.
ip host mediaserver-backup ###.###.###.### # IP Address for secondary media server.
```

Step 6 Configure the dial-peers:

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


# Configure 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 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



#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



#Configure the Switch leg where
 # preference is used to distinguish between sides.
 # max-conn is used prevent overloading of 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 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 CVP1, SideA
 session transport tcp
 voice-class codec 1
 voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
 dtmf-relay rtp-nte
 no vad


dial-peer voice 70022 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 CVP2, SideA
 session transport tcp
 voice-class codec 1
 voice-class sip options-keepalive up-interval 12 down-interval 65 retry 2
 dtmf-relay rtp-nte
 no vad


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


dial-peer voice 70024 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 CVP2, 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 section is only for reference. You must configure Hardware resources using
Unified Communications Domain Manager.
# Configure the voice-cards share the DSP resources located in Slot0
voice-card 0
dspfarm
dsp services dspfarm
voice-card 1
dspfarm
dsp services dspfarm
voice-card 2
dspfarm
dsp services dspfarm
voice-card 3
dspfarm
dsp services dspfarm
voice-card 4
dspfarm
dsp services dspfarm

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

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

# Configure DSPFarms for Conference, MTP and Transcoder
dspfarm profile 1 conference
codec g711ulaw
codec g711alaw
codec g729r8
maximum sessions 24
associate application SCCP

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

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

Note Universal transcoder is only needed for cases where you engage the G.729 caller to G.729 only agent with IVR in middle and performs any supplementary services or use features like whisper announcement or agent greeting. If both the agent and caller are using G.729, transcoding is not required. .

Step 8 (Optional) Configure the SIP Trunking:

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

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

Step 9 Configure Incoming PSTN Sip Trunk Dial Peer

```
dial-peer voice 70000 voip
 description Incoming Call From PSTN SIP Trunk
 incoming called-number xxxx…… # Customer specific incoming called-number pattern
 voice-class sip rel1xx disable
 dtmf-relay rtp-nte h245-signal h245-alphanumeric
 codec g711ulaw
 no vad
```

Step 10 Configure ASR TTS:

```
#Configure primary server
ip host asr-en-us <ASR server ip>
ip host tts-en-us <TTS server hostname>

voice class uri TTS sip
pattern tts@<TTS server ip>

voice class uri ASR sip
pattern asr@<ASR server hostname>

ivr asr-server sip:asr@<ASR server hostname*>
ivr tts-server sip:tts@<TTS server hostname*>

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

dial-peer voice 6 voip
description FOR TTS calls
```

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

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

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

Step 11 Configure SNMP

```
snmp-server community <string name> ro
```

Step 12 Configure Back-office

Note Example here is for Internal number that is dialed is 82009999 and converting the Internal number to the PSTN number : 2142009999

Example:

```
voice translation-rule 2
rule 1 /^8200/ /214200

voice translation-profile Xform
translate called 2
```

Note Ensure that you configure dial-peers for each CVP server

```
dial-peer voice 2 voip
description out dial-peer CC pilot dial-peer
translation-profile outgoing Xform
destination-pattern 8200T
session protocol sipv2
session target ipv4:<IP address of CVP Server>
session transport tcp
voice-class codec 1
dtmf-relay rtp-nte
```

Configure Cisco Unified Communications Manager

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 Unified Communications Manager Groups

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

Before you configure a Unified Communications Manager Group, you must configure the Unified Communications Managers that you want to assign as members to that group.

Procedure

Step 1 Login to the **Cisco Unified Communication Manager Administration** page, choose **System** > **Server**.

Step 2 Make sure that you configure both the Publisher and Subscriber.

a) Click **Add New**.
b) Select appropriate Server Type Eg: CUCM Voice/Video Select **Next**.
c) Enter the **Host Name/IP Address**.
d) Click **Save**.

Step 3 Choose **System** > **Cisco Unified CM**.

Step 4 Click **Find**.

Step 5 Make sure that you configured both the Publisher and Subscriber.

Step 6 Choose **System** > **Cisco Unified CM Group**.

Step 7 Add both Cisco Unified Communications Managers to the Default Unified Communications Manager Group. Select **Default** and from the Available Cisco unified communication managers select both Publisher and Subscriber to Selected Cisco Unified Communications Managers

Step 8 Click **Save**.

Set Up CTI Route Point

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

Procedure

Step 1 Choose **Device** > **CTI Route Point**.

Step 2 Click **Add New**.

Step 3 Use the wildcard string **XXXXX** to represent the digits of the dialed number configured on Unified CCE.

Note For example, the preconfigured dialed number in the Unified CCE for an agent phone is 10112.

Step 4 Select the appropriate device pool.

Step 5 Click **Save**.

Set Up Trunk

Complete the following procedure to configure a trunk for the Unified CVP Servers.

Procedure

Step 1 Choose **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 In the Device Name field, enter a name for the SIP trunk.

Step 5 In the Description field, enter a description for the SIP trunk.

a) Enter the SIP Trunk name in the Device Name field.
b) Select the appropriate Device Pool.

Step 6 Click **Next**.

Step 7 In the Trunk Configuration window, enter the appropriate settings:

a) Uncheck the **Media Termination Point** Required check box.
b) Enter the **Destination Address**.
c) Select the appropriate SIP Trunk Security Profile
d) From the **SIP Profile** drop-down list, choose **Standard SIP Profile**.
e) From the DTMF Signaling Method drop-down list, choose **RFC 2833**.

Step 8 Click **Save**.

Set Up Application User

Procedure

Step 1 Choose **User Management** > **Application User**.

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

Step 3 Enter the User ID that you entered in Set Up Enterprise Parameters , on page 73. Unified CCE defines the user ID as pguser.

Step 4 Enter a **cisco** in the Password field of your choice.

Note If you change this user ID or password in Unified CCE, you must also change the Unified Communications Manager application user configuration.

Note To change the JTAPI password on the CUCM configuration page:

a. Open the peripheral Gateway Setup in PG Machine.

b. Edit the CUCM PG.

c. Set the same password for the user as previously set in Step 4.

Step 5 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 6 Associate the CTI route points and the phones with the application user.

Step 7 Click **Save**.

Set Up SIP Options

Procedure

Step 1 Select **Device** > **Device Settings** > **SIP Profile**.

Step 2 Enter values for the mandatory fields.

Step 3 Select the **Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"** check box.

Step 4 Associate this SIP profile on the trunk.

Set Up Route Pattern

Procedure

Step 1 Choose **Call Routing** > **Route Hunt** > **Route Pattern**.

Step 2 Add a route pattern for the Unified CVP routing clients as follows:

a) Click **Add New**.
b) In the **Route Pattern** field, enter `7777777777!`
c) In the **Gateway/Route List** field, choose **SIPTRK_to_CVP_1**.
d) Click **Save**.

Step 3 Add a route pattern for the Cisco Unified Communications Manager routing client.

a) Click **Add New**.
b) In the **Route Pattern** field, enter `8881111!`
c) In the **Gateway/Route List** field, choose **SIPTRK_to_CVP_1**.
d) Click **Save**.

Note These route patterns must match the network VRU label defined in Unified CCE.

Set Up Conference Bridge

Procedure

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

Step 2 Add a conference bridge for each ingress/VXML combination gateway in the deployment.

Step 3 In the Conference Bridge name field, enter a unique identifier for the conference bridge name that coincides with the configuration on the gateway.

Step 4 Click **Save**.

Step 5 Click **Apply Config**.

Set Up Media Termination Point

Procedure

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

Step 2 Add a media termination point for each ingress/VXML combo gateway in the deployment.

Step 3 In the Media Termination Point Name field, enter a media termination point name for each ingress/VXML combo gateway in the deployment.

Step 4 Click **Save**.

Step 5 Click **Apply Config**.

Set Up Transcoder

Procedure

Step 1 Choose **Media Resources** > **Transcoder**.
Step 2 Add a transcoder for each ingress/VXML combo gateway in the deployment.
Step 3 In the Device Name field, enter a unique identifier for the transcoder that coincides with the configuration on the gateway.
Step 4 Click **Save**.
Step 5 Click **Apply Config**.

Set Up Media Resource Group

Complete the following procedure to configure a media resource group for conference bridge, media termination point, and transcoder.

Procedure

Step 1 Choose **Media Resources** > **Media Resource Group**.
Step 2 Add a Media Resource Group for Conference Bridges.
Step 3 Select all the hardware conference bridge resources configured for each ingress/VXML combination gateway in the deployment and add them to the group.
Step 4 Click **Save**.
Step 5 Choose **Media Resources** > **Media Resource Group**.
Step 6 Add a Media Resource Group for Media Termination Point.
Step 7 Select all the hardware media termination points configured for each ingress/VXML combination gateway in the deployment and add them to the group.
Step 8 Click **Save**.
Step 9 Choose **Media Resources** > **Media Resource Group**.
Step 10 Add a Media Resource Group for Transcoder.
Step 11 Select all the transcoders configured for each ingress/VXML combination gateway in the deployment and add them to the group.
Step 12 Click **Save**.

Set Up and Associate Media Resource Group List

Complete the following procedure to configure and associate a media resource group list. Add the media resource group list to the following devices and device pool.

Procedure

Step 1 Choose **Media Resources** > **Media Resource Group List**.
Step 2 Add a Media Resource Group list and associate all of the media resource groups.
Step 3 Click **Save**.
Step 4 Choose **System** > **Device Pool**.
Step 5 Click **Default**.
Step 6 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2.
Step 7 Click **Save**.
Step 8 Click **Reset**.
Step 9 Choose **Device** > **CTI Route Point**.
Step 10 Click the configured CTI Route Point. For more information, see Set Up CTI Route Point , on page 69.
Step 11 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2
Step 12 Click **Save**.
Step 13 Click **Reset**.
Step 14 Choose **Device** > **SIP Trunk**.
Step 15 Click the configured SIP Trunk for. For more information, see Set Up Trunk , on page 69.
Step 16 From the Media Resource Group List drop-down list, choose the media resource group added in Step 2
Step 17 Click **Save**.
Step 18 Click **Reset**.

Set Up Enterprise Parameters

Procedure

Step 1 Choose **System** > **Enterprise Parameter**.
Step 2 Configure the Cluster Fully Qualified Domain Name.

Example:

ccm.cce.icm

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

Configure Mobile Agent

Complete the following procedure to configure CTI ports for Unified Mobile Agent.

Procedure

Step 1 In Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Click **Add a New Phone**.

Step 3 Select **CTI Port** from the **Phone Type** drop-down list.

Step 4 Click **Next**.

Step 5 In Device Name, enter a unique name for the local CTI Port pool name; click **OK** when finished.

Using the example naming convention format LCPxxxxFyyyy:

a) LCP identifies the CTI Port as a local device.
b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
c) yyyy is the local CTI Port.

The name LCP5000F0000 would represent CTI Port: 0 in a local CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.

Step 6 In Description, enter text identifying the local CTI Port pool.

Step 7 Use the **Device Pool** drop-down list to choose the device pool to which you want network CTIPort pool assigned. (The device pool defines sets of common characteristics for devices.)

Step 8 Click **Save**.

Step 9 Highlight a record and select Add a New DN.

Step 10 Add a unique directory number for the CTI port you just created.

Step 11 When finished, click **Save** and **Close**.

Step 12 Repeat the preceding steps to configure the network CTI Port pool.

Step 13 In Device Name, enter a unique name for the local CTI Port pool name; click **OK** when finished.

Use the example naming convention format RCPxxxxFyyyy, where:

a) RCP identifies the CTI Port as a network device.
b) xxxx is the peripheral ID for the Unified Communications Manager PIM.
c) yyyy is the network CTI Port.

The name RCP5000F0000 would represent CTI Port: 0 in a network CTI Port pool for the Unified Communications Manager PIM with the peripheral ID 5000.

Step 14 In Description, enter text identifying the network CTI Port pool.

Step 15 Use the **Device Pool** drop-down list to choose the device pool to which you want network CTI Port pool assigned. (The device pool defines sets of common characteristics for devices.)

Step 16 Click **Save**.

Step 17 Highlight a record and select **Add a New DN**.

Step 18 Add a unique directory number for the CTI port you just created.

Step 19 When finished, click **Save** and **Close**.

Configure Local Trunk

Complete the following procedure to configure Unified Communications Manager for Local Trunk.

Procedure

Step 1 From Unified Communications Manager Administration choose **System** > **Location info** > **Location**.

Step 2 Click **Find** to list the locations and add new ones with appropriate bandwidth (8000).

Step 3 For the branch phones, configure each phone so that it is assigned the branch location for that phone.

a) Choose **Device > Phone**.
b) Click **Find** to list the phones.
c) Select a phone and set the Location field.

Step 4 Verify that the Cisco AXL Web Service is started and that an Application User is defined and has a role of Standard AXL API Access.

a) Select **Cisco Unified Serviceability** from the **Navigation** drop-down list and click **Go**.
b) Navigate to **Tools** > **Control Center** > **Feature Services** .
c) Start the Cisco AXL Web Service, if it is not started.
d) From Unified Communications Manager Administration, choose **User Management > Application User**. Verify you have a user with the role of Standard AXL API Access, or create a new one and add that user to a group that has the role of Standard AXL API Access.

Deploy SIP Trunk

Complete the following procedure to deploy the SIP trunk for local trunk:

Procedure

Step 1 Using Unified Communications Manager, create a SIP trunk toward the SIP proxy server and select the Phantom location.

Step 2 Create a SIP trunk for each ingress gateway and make the location of these ingress TDM-IP gateways the actual branch location.

Step 3 Create a route pattern pointing the Network VRU Label of the Unified Communications Manager routing client to the SIP trunk toward the SIP proxy.

The SIP proxy should route the Network VRU label of the Unified Communications Manager routing client to the Unified CVP Servers.

Step 4 For any IP-originated calls, associate the Unified Communications Manager route pattern with the SIP trunk.

Step 5 Using the Unified Communications Manager Administration, choose **Device > Device Settings > SIP Profile > Trunk Specific Configuration > Reroute Incoming Request to new Trunk based on > Call-Info header with the purpose equal to x-cisco-origIP**.

Step 6 Associate the new SIP profile with the SIP trunk and each ingress gateway.

Configure Outbound Dialer

Complete the following procedure to configure Unified Communications Manager:

Procedure

Step 1 Log in to the Unified Communications Manager administration page.

Step 2 Select **Devices** > **Trunk**.

Step 3 Create a SIP trunk to Outbound gateway.

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 Support for Multiline Agent Control

To enable reporting and control of secondary lines, follow these configuration steps on Unified Communications Manager. This is required for deployments that have agents using phones that require Join Across Line (JAL) to be enabled.

Note Use of JAL and DTAL phone features is deprecated. Do not use these features in new deployments.

Multiline Agent Control supports a maximum of four lines per phone, one ACD line and up to three non-ACD lines.

Note Unified CCE supports shared lines for ACD lines but does not support for Non ACD lines.

Several agents cannot share a common extension on their phones. However, one agent can have two phones that share a common second line. The agent cannot sign in on both phones at the same time.

Procedure

Step 1 Enable the Application User for the agent peripheral with the role of **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** to support phones that require Join Across Line setting.

Step 2 Configure all agent phones with the following parameters:

- **Busy Trigger: 1**
- **Maximum Number of Calls: 2**

Configure Caller-Specific Music on Hold

Upload audio file

Follow this procedure to upload an audio file in an existing node or new node in a Cisco Unified Communications Manager cluster.

If you are uploading to a new node, you must first configure a new and dedicated Music on Hold node that can have only two Cisco Unified Communications Manager services running: Cisco Call Manager, and Cisco IP Voice Media Streaming Application. Additionally, the Cisco IP Voice Media Streaming Application service must be deactivated in all of the other nodes in the Cisco Unified Communications Manager cluster that contains the dedicated Music on Hold node. For more information, see Installing Cisco Unified Communications Manager.

Procedure

Step 1 Log in to the Cisco Unified Communications Manager Administration page.

Step 2 Click the **Media resources** tab, and then click **MOH Audio File Management**.

Step 3 In the MOH Audio File Management page, click **Upload File**.

Step 4 In the Upload File window, click **Browse**, select the audio file that you want to set for Music on Hold, and then click **Open**.

Step 5 Click **Upload File**.

The audio file is now available for use as a Music on Hold audio source.

What to do next

Configure the uploaded audio file so that it can be used as an audio source for Music on Hold.

Configure audio source

Procedure

Step 1 In the Cisco Unified Communications Manager Administration page, click **Media resources** tab, and then click **Music On Hold Audio Source**.

Step 2 Click **Add new**.

Step 3 In the MOH Audio Stream Number field, enter a number that you want to assign to the audio file. You cannot choose a number that has already been assigned to another audio file.

Step 4 In the MOH Audio Source file drop-down menu, choose the audio file that you want to configure as the MoH audio source.

Step 5 (Optional) The MOH Audio Source Name field automatically populates the name of the audio file that you chose in the previous step. You can edit the name of the audio file that you selected.

Step 6 Click **Save**.

What to do next

Configure the audio source in the Unified CCE routing script.

Configure Unified CCE routing script

Procedure

Step 1 Log in to the Unified CCE Administrator workstation.

Step 2 Open the Script Editor.

Step 3 Open the script in which you want to set the caller specific Music on Hold.

Step 4 Set the call variable *SIPHeader* with the value `X-cisco-moh-source~mod~<User Hold MoH Audio File number>,<Network Hold MoH Audio File number>.`

Example:

For example, X-cisco-moh-source~mod~6,7; where 6 and 7 are the numbers that you assigned to the audio file. In this example, the audio file assigned for number 6 is played when the call is placed on user hold, and the audio file assigned for number 7 is played when the call is placed on network hold.

Note
- List the new call variable after a Dialed Number (DN) or CallingLineID node. This ensures that the call is for a particular DN, or from a particular Calling Line ID.
- If only one audio file is specified, the same file is used for both user hold and network hold.
- If the audio stream that you specified is not present in the Cisco Unified Communications Manager cluster, then the default Music on Hold of the device plays.

Step 5 Click **Save**.

The audio file is now configured as the source audio file that will play for caller specific Music on Hold.

Configure Cisco Finesse

Configure Contact Center Enterprise CTI Server Settings

Configure the A Side and B Side CTI servers on the primary Finesse server.

Procedure

Step 1 If you are not already signed in, sign in to the administration console on the primary Finesse server:

http://FQDN hostname, or IP address of Finesse server/cfadmin

Step 2 Sign in with the Application User credentials defined during installation.

Step 3 In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

Field	Description
A Side Host/IP Address	Enter the hostname or IP address of the A Side CTI server. This value is typically the IP address of the Peripheral Gateway (PG). The CTI server runs on the PG.
A Side Port	Enter the port number of the A Side CTI server. The value of this field must match the port configured during the setup of the A Side CTI server.
Peripheral ID	Enter the ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A Side and B Side CTI servers.
B Side Host/IP Address	Enter the hostname or IP address of the B Side CTI server.
B Side Port	Enter the port of the B Side CTI server. The value of this field must match the port configured during the setup of the B Side CTI server.
Enable SSL encryption	Check this box to enable secure encryption.

Step 4 Click **Save**.

Configure Contact Center Enterprise Administration and Data Server Settings

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

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

Procedure

Step 1 Sign in to the administration console.

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

Field	Description
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server. For example, **abcd12-5-aw-a**.
Backup Host/IP Address	The hostname or IP address of the backup Unified CCE Administration & Data Server. For example, **abcd12-5-aw-b**.
Database Port	The port of the Unified CCE Administration & Data Server. The default value is 1433. **Note** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the Finesse administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
AW Database Name	The name of the AW Database (AWDB). For example, **ucceinstance_awdb**.
Domain	The domain name of the AWDB. For example, **cisco.com**.
Username	The username required to sign in to the AWDB. **Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user. If you do not specify a domain, this user must be an SQL user.
Password	The password required to sign in to the AWDB.

Step 3 Click **Save**.

Configure Cluster Settings

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

Procedure

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

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

Step 3 Click **Save**.

Restart Cisco Finesse Tomcat

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

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

Procedure

Step 1 Access the CLI and run the following command:

utils service restart Cisco Finesse Tomcat

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

Check Replication Status

Procedure

Step 1 Access the CLI on the primary Finesse server.

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

Step 3 Run the following command:

utils dbreplication runtimestate

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

Ensure Agents Have Passwords

Agents who do not have a password defined in Unified CCE Configuration Manager cannot sign in to Finesse.

Agent password is an optional field in Unified CCE, but it is mandatory for Cisco Finesse.

For agents who do not have passwords, you must perform the following steps:

Procedure

Step 1 Launch Unified CCE Configuration Manager.

Step 2 Locate the record for the agent (Agent Explorer > Agent tab).

Step 3 Enter a password, and save the record.

Ensure Logout Non-Activity Time for Agents is Configured

The Logout non-activity time specifies how long an agent can remain inactive in the Not Ready state before that agent is signed out of Finesse.

For agents who use the Task Routing interface on Finesse for non-voice tasks, set the Logout non-activity time to blank.

Perform the following steps to configure Logout non-activity time for an agent.

Procedure

Step 1 Launch the Unified CCE Configuration Manager.

Step 2 Launch Agent Desk Settings List (**Tools** > **List Tools**).

Step 3 Select **Agent Desk Settings List**.

Step 4 In the Logout non-activity time field, enter the number of seconds of agent inactivity while in the Not Ready state before the system software signs the agent out. You can enter a value between 10 seconds and 7200 seconds.

Step 5 Click **Save**.

The modified settings are applied to all of the agents who use these agent desktop settings.

Browser Settings for Internet Explorer

If Internet Explorer is used to access the Finesse desktop, certain settings must be configured in the browser to ensure all features of Finesse work properly.

1. Disable pop-up blockers.

   Finesse does not support Compatibility View. When the desktop is running in Compatibility View, Internet Explorer renders in the standard mode for that version.

2. Configure the following privacy and advanced settings:
   a. From the browser menu, select **Tools** > **Internet Options**.
   b. Click the **Privacy** tab.
   c. Click **Sites**.
   d. In the Address of website box, enter the domain name for the Side A Finesse server.
   e. Click **Allow**.
   f. In the Address of website box, enter the domain name for the Side B Finesse server.
   g. Click **Allow**.
   h. Click **OK**.

3. You must enable the following security settings to allow users to sign in:
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked as safe for scripting
   - Active scripting

   To enable these settings:

   a. From the Internet Explorer browser menu, select **Tools** > **Internet Options**.
   b. Click the **Security** tab.
   c. Click **Custom level**.
   d. Under ActiveX controls and plug-ins, select **Enable** for **Run ActiveX controls and plug-ins** and **Script ActiveX controls marked safe for scripting**.
   e. Under Scripting, select **Enable** for **Active Scripting**.

Note If the customer is using self-signed CA (Certificate Authority) and their agents use the server's FQDN, there should not be any certificate errors or warnings when connecting to Finesse over HTTPS.

Browser Settings for Firefox

Complete the following steps to ensure Finesse behaves as expected when it is not the active window.

Procedure

Step 1 Open Firefox and enter **`about:config`** in the address bar.
A warning page appears that states, `This might void your warranty!`.

Step 2 Click **I'll be careful, I promise!**.

Step 3 In the **Search** field, enter **`dom.disable_window_flip`**.

Step 4 Double-click **dom.disable_window_flip** to set the value to *false*.

Step 5 Restart Firefox.

Ensure Agents Can Sign in to Desktop

After the system administrator defines configuration settings and restarts services, agents who have passwords and operational handsets can sign in to the Finesse Agent Desktop.

Note Finesse agents can enter either their `AgentID` or `Login name` (in the **Username** field of the desktop login screen) to sign in. Ensure that each agent's `AgentID` and `Login name` are unique across both sets of data. If one agent's `AgentID` matches another agent's `Login name`, neither agent can sign in.

Note After you restart Finesse, it takes approximately 6 minutes for all server-related services to restart. Therefore, you should wait 6 minutes before you attempt to sign in to the desktop.

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

Procedure

Step 1 Enter the following URL in the address bar of your browser:

http://*FQDN of Finesse server*/desktop

Step 2 If you installed the language pack ES file, you can select the language you want to appear on the desktop from the language selector drop-down list. If you did not install the language pack ES file, the language selector drop-down list does not appear in the user interface.

Note If you installed the language pack ES file, you can also select a language by passing the locale as part of the URL (for example, http://*FQDN of Finesse server*/desktop?locale=fr_FR) or by changing your browser preferred language. The default language is English (en_US).

Step 3 Enter your Username, Password, and Extension, and then click **Sign In**.

If your agent is signed into the Agent Desktop in Single Sign-On Mode or Hybrid Mode, refer to the sections *Sign In to Finesse Desktop Single Sign-On Mode* or *Sign In to Finesse Desktop Hybrid Mode* in the *Cisco Finesse Desktop User Guide for Unified Contact Center Enterprise.*

Trust Self-Signed Certificate

Trust the self-signed certificate provided by Finesse to eliminate browser warnings each time you sign in to the administration console or agent desktop.

If you are not using HTTPS or if you uploaded a CA certificate, you can skip this procedure.

Procedure

Step 1 In your browser, enter the URL for the administration console (https://*hostname of primary server:portnumber*/cfadmin) or the agent desktop (https://*hostname of primary server*).

Step 2 Perform the steps in the following table for the browser you are using.

Option	Description
If you use Internet Explorer:	**a.** A page appears that states there is a problem with the website's security certificate. Click **Continue to this website (not recommended)**. This action opens the sign in page for

Option	Description
	the administration console (or agent desktop). A certificate error appears in the address bar of your browser. **b.** Click **Certificate Error**, and then click **View Certificates** to open the Certificate dialog box. **c.** On the Certificate dialog box, click **Install Certificate**. This action opens the Certificate Import Wizard. **Note** If you use Internet Explorer 11, you must add Finesse to your trusted sites before the Install Certificate option appears (**Internet Options** > **Security** > **Trusted Sites** > **Sites**). After you click **Install Certificate**, under **Store Location**, select **Current User** to install the certificate for the current user only, or select **Local Machine** to install the certificate for all Windows users who use this computer. **d.** Click **Next**. **e.** Select **Place all certificates in the following store**, and then click **Browse**. **f.** Select **Trusted Root Certification Authorities**, and then click **OK**. **g.** Click **Next**. **h.** Click **Finish**. **i.** If a Security Warning dialog box appears that asks if you want to install the certificate, click **Yes**. A Certificate Import dialog box that states the import was successful appears. **j.** Click **OK**. **k.** Enter your credentials, and then click **Sign In**.
If you use Firefox:	**a.** A page appears that states this connection is untrusted. **b.** Click **I Understand the Risks**, and then click **Add Exception**. **c.** On the Add Security Exception dialog box, ensure the **Permanently store this exception** check box is checked. **d.** Click **Confirm Security Exception**. The page that states this connection is untrusted automatically closes and the administration console (or agent desktop) loads. **e.** Enter your credentials, and then click **Sign In**. **f.** For the agent desktop only, an error appears that states Finesse cannot connect to the Cisco Finesse Notification Service and prompts you to add a security exception for the certificates issued by the Finesse server.

Option	Description
	Click **OK**.

Obtain and Upload CA Certificate

Note This procedure only applies 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 Finesse.

To eliminate browser security warnings each time you sign in, obtain an application and root certificate signed by a Certificate Authority (CA). Use the Certificate Management utility from Cisco Unified Communications Operating System Administration.

To open Cisco Unified Communications Operating System Administration, enter the following URL in your browser:

https://*hostname of primary UCCX server*/cmplatform

Sign in using the username and password for the Application User account created during the installation of Finesse.

Note You can find detailed explanations in the Security topics of the *Cisco Unified Communications Operating System Administration Online Help*.

Procedure

Step 1 Generate a CSR.

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

Note To avoid certificate exception warnings, you must access the servers using the Fully Qualified Domain Name (FQDN).

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 Generate and download a CSR for the secondary Finesse server.

To open Cisco Unified Operating System Administration for the secondary server, enter the following URL in the address bar of your browser:

https://*hostname of secondary UCCX server*/cmplatform

Step 4 Use the CSRs to obtain the CA root certificate, intermediate certificate, and signed application certificate from the Certificate Authority.

Note To set up the certificate chain correctly, you must upload the certificates in the order described in the following steps.

Step 5 When you receive the certificates, select **Security** > **Certificate Management** > **Upload Certificate**.

Step 6 Upload the root certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the root certificate file.
c) Click **Upload File**.

Step 7 Upload the intermediate certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat-trust**.
b) In the **Upload File** field, click **Browse** and browse to the intermediate certificate file.
c) Click **Upload File**.

Step 8 Upload the application certificate.

a) From the **Certificate Purpose** drop-down list, select **tomcat**.
b) In the **Upload File** field, click **Browse** and browse to the application certificate file.
c) Click **Upload File**.

Step 9 After the upload is complete, sign out from the Platform Admin page of Finesse.

Step 10 Restart Cisco Tomcat on the primary Unified CCX node.

Step 11 Restart Cisco Finesse Tomcat on the primary Unified CCX node.

Step 12 Restart Cisco Unified Intelligence Center Reporting Service.

Step 13 Restart Unified CCX Notification Service.

Note It is recommended to delete the self-signed certificates from the clients certificate store. Then close the browser, relaunch, and reauthenticate.

Step 14 Upload the application certificate to the secondary Unified CCX server.

You do not need to upload the root and intermediate certificates to the secondary Unified CCX server. After you upload these certificates to the primary server, they are replicated to the secondary server.

Step 15 Restart Cisco Tomcat and Cisco Finesse Tomcat on the secondary Unified CCX node.

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 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 Internet Explorer

In environments where group policies are enforced via the Active Directory domain, the root certificate can be added automatically to each user's Internet Explorer. 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 Internet Explorer 11.

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 Internet Explorer.

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 Browser

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 Click **Trusted Root Certification Authorities** tab.

Step 4 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 5 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:

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

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.

Browser Settings for Internet Explorer

To ensure all features of Finesse work properly in Internet Explorer, you must:

1. Disable pop-up blockers.
2. Configure the following privacy and advanced settings:
   a. From the browser menu, select **Tools** > **Internet Options**.
   b. In the **Privacy** tab, click **Sites**.
   c. In the Address of website box, enter the domain name for the Side A Finesse server.
   d. Click **Allow**.
   e. In the Address of website box, enter the domain name for the Side B Finesse server.
   f. Click **Allow** > **OK**.
3. Enable the following security settings to allow users to sign in:
   - Run ActiveX controls and plug-ins
   - Script ActiveX controls marked as safe for scripting
   - Active scripting

   To enable these settings:
   a. From the Internet Explorer browser menu, click **Tools** > **Internet Options**.
   b. In the **Security** tab, click **Custom level**.
   c. Under ActiveX controls and plug-ins, select **Enable** for **Run ActiveX controls and plug-ins** and **Script ActiveX controls marked safe for scripting**.
   d. Under Scripting, select **Enable** for **Active Scripting**.

Note If you are using self-signed or CA-signed certificates and the server's FQDN, there should not be any certificate errors or warnings when connecting to Cisco Finesse over HTTPS.

Browser Settings for Firefox

Complete the following steps to ensure Finesse responds as expected when it is not the active window:

Procedure

Step 1 Open Firefox and enter **about:config** in the address bar.
Step 2 On the warranty page, click **I accept the risk!**.
Step 3 In the **Search** field, enter `dom.disable_window_flip`.
Step 4 Double-click **dom.disable_window_flip** to set the value to *false*.
Step 5 Restart Firefox.

Browser Settings for Chrome

Ensure that you disable the **Automatic tab discarding** feature in Chrome (version 74 and earlier) to avoid exiting the Finesse desktop tab when the system memory is low.

Procedure

Step 1 Open Chrome and enter **chrome://flags/#automatic-tab-discarding** in the address bar.
Step 2 Press **Enter**.
Step 3 Select **Disabled** from the drop-down list.
Step 4 Click **Relaunch Now**.

Configure DNS on Clients

Note This procedure is required for uncommon environments where non-hierarchical DNS configuration exists. If your environment has hierarchical DNS configuration, you do not need to perform this procedure. This procedure applies to clients that use a Windows operating system. For information about configuring DNS on Mac clients, see your Apple documentation (www.apple.com/mac).

Configuring DNS on client computers allows the clients to resolve the fully-qualified domain name (FQDN) of the active Finesse server during a failover.

Procedure

Step 1 Go to **Control Panel** > **Network and Internet** > **Network and Sharing Center**. (Open the Control Panel, enter Network Connections in the search bar, and then click **View network connections**.)

Step 2 Click the appropriate network connection.
A dialog box showing the status of the connection appears.

Step 3 Click **Properties**.

Step 4 On the Networking tab, select Internet protocol version 4 (TCP/IPv4) or Internet protocol version 6 (TCP/IPv6) if the client is IPV6, and then click **Properties**.

Step 5 Click **Advanced**.

Step 6 On the DNS tab, under DNS server addresses, in order of use, click **Add**.

Step 7 Enter the IP address of the DNS server that was entered during installation and click **Add**.

Step 8 If a secondary DNS was entered during installation, repeat Step 5 and Step 6 to add its IP address.

Live Data Reports

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

Prerequisites for Live Data

Before you add Live Data reports to the desktop, you must meet the following prerequisites:

- You must have the Live Data reports configured and working in Cisco Unified Intelligence Center.
- You must use either HTTP or HTTPS for both Cisco Unified Intelligence Center and Finesse. You cannot use HTTP for one and HTTPS for the other. The default setting for both after a fresh installation is HTTPS. If you want to use HTTP, you must enable it on both Cisco Unified Intelligence Center and Finesse. For information about enabling HTTP for Cisco Unified Intelligence Center, see the *Administration Console User Guide for Cisco Unified Intelligence Center* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.
- Ensure that user integration synchronization is enabled for Cisco Unified Intelligence Center. For more information, see the *Administration Console User Guide for Cisco Unified Intelligence Center* .
- If your deployment uses HTTPS, you must upload security certificates to the Finesse, Cisco Unified Intelligence Center, and Live Data servers depending your deployment:

On Server	Import Certificates From
Finesse	Live Data and Cisco Unified Intelligence Center
Live Data	None required
Cisco Unified Intelligence Center	Live Data

Finesse, Cisco Unified Intelligence Center, and Live Data are installed with self-signed certificates. However, if you use the self-signed certificates, agents and supervisors must accept certificates in the Finesse desktop when they sign in before they can use the Live Data gadget. To avoid this requirement,

you can provide a CA certificate instead. You can obtain a CA certificate from a third-party certificate vendor or produce one internal to your organization.

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 Sign in to the Finesse administration console (`https://FQDN of Finesse server:Port Number(8445)/cfadmin`), in which FQDN refers to the fully qualified domain name.

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**.

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.

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 Sign in to the Finesse administration console.

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. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

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.

Add Live Data Reports to Team 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 desktop layout of a specific team. 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 Sign in to the Finesse administration console.

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. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

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 Click the **Team Resources** tab.

Step 6 Select the team from the list of teams for which you want to add the report.

Step 7 In the Resources for <team name> area, click the **Desktop Layout** tab.

Step 8 Check the **Override System Default** check box.

Step 9 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 10 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 11 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 12 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.

Modify Live Data Stock Reports for Finesse

This procedure describes how to modify the Live Data stock reports in Cisco Unified Intelligence Center and add the modified report to the Finesse 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.

Note To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Cisco Unified Intelligence Center.

Procedure

Step 1 Sign in to the Finesse administration console.

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

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

Step 4 Copy the gadget URL for the report you want to modify from the Finesse default layout XML and paste it into a text editor.

Example:

If you want to modify the Agent Report for HTTPS, copy the following URL and paste it into a text editor:

```
<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 In Cisco Unified Intelligence Center, in Edit view of the report, select the view for which you want to create a gadget URL and then click **Links**.

The HTML Link field displays the permalink of the customized report.

Step 6 Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor. Then copy the viewId value from this link into the desired view.

Example:

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

Step 7 Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.

Step 8 Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.

Step 9 Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

Note After you add the 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 the need to scroll.

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.

Initial Configuration Troubleshooting

If	Then
The administration console does not load after a fresh installation.	1. Clear your browser cache (delete browsing history and cookies). 2. If the problem persists, restart the Cisco Finesse Tomcat service or restart the Finesse server.

If	Then
Agents cannot sign in to the desktop after a fresh installation.	**1.** Verify that a valid domain was configured during installation and that forward and reverse DNS are set up correctly. To check whether DNS was configured during installation, check the install.log for the following: InstallWizard|USER_ACTION_BTN_PUSH: Screen = DNS Client Configuration, button pushed = No|<LVL::Info The preceding message indicates that DNS was not configured during the installation. Reinstall Finesse and configure the DNS with a valid domain. **2.** Verify that the agent is configured in Unified CCE. **3.** Verify that the AWDB is configured correctly. **a.** Check the realm.log for the following line: "ERROR com.cisco.ccbu.finesse.realms.ccerealm.CCERealmConfig - Cannot connect to any AWDB! Ensure that at least one AWDB is configured properly and running!" This line indicates that Finesse cannot connect to the AWDB. **b.** Check that the values entered in the Contact Center Enterprise Administration & Data Server Settings gadget are correct. • Verify that the username entered is a Windows domain user. • Verify that the username is not prepended with the domain (for example, domain\username). • Verify that the port configured is open to the Finesse server. **c.** Check that the AWDB is set up correctly and running. • The AWDB SQL server must use Windows authentication. • Verify that the AWDB server is up and that the Distributor service is running. **4.** Restart Cisco Finesse Tomcat on the primary and secondary Finesse servers. **5.** Verify that the agent's device is properly configured in Unified Communications Manager and is active.