Packaged CCE Administration

Getting Started

Sign In

You must do post installation configurations to sign in to the Unified CCE Administration. For more information, see Post Installation Configuration .

Sign in to Unified CCE Administration at https://<IP Address>/cceadmin. <IP Address> is the address of the Side A or B Unified CCE AW or optional external HDS.

Note Users are logged out of the Unified CCE Administration console automatically after 30 minutes of inactivity.

Administrators

Administrators sign in using their Active Directory credentials. For **username**, use the *user@domain.com* format.

Supervisors

Supervisors on an IPv6 network sign in to Unified CCE Administration at `https://<FQDN>/cceadmin`. *<FQDN>* is the fully qualified domain name of the Side A or B CCE AW or optional external HDS.

Supervisors sign in using their Active Directory (*user@domain.com*) or single sign-on credentials. If supervisors are enabled for single sign-on, after entering their username they are redirected to the Identity Provider sign-in screen to enter their credentials. Supervisors are redirected to Unified CCE Administration after successfully signing in.

Languages

If the Language Pack is installed, the Sign-In window includes a Language drop-down menu, showing more than a dozen languages. English is the initial and the default language. Select any other language to see the user interface and the online help in that language. The system retains your choice for subsequent sign-ins until you change it again.

Single Sign-On Log Out

For a complete logout from all applications, sign out of the applications and close the browser window. In a Windows desktop, log out of the Windows account. In a Mac desktop, quit the browser application.

Note Users enabled for single sign-on are at risk of having their accounts misused by others if the browser is not closed completely. If the browser is left open, a different user can access the application from the browser page without entering credentials.

System Interface

Packaged CCE user interface enables you to configure the application through one window. The landing page has a left navigation bar and a card view which contains all the configuration options. What you see after a successful sign-in depends on your role.

The left navigation bar consists of the following menus:

- Overview
- Infrastructure
- Organization
- Users
- Desktop
- Capacity

The following menus appear as cards:

- Infrastructure Settings
- Call Settings
- User Setup
- Organization Setup
- Bulk Import

- Desktop Settings
- Features
- Email and Chat

  (Available only when ECE Web Server is added to the **Infrastructure** > **Inventory** page on the Unified CCE Administration.)

Note The Unified CCE Administration interface also provides access to HTML-based online help for users and administrators. Click on the help button (**?**) on any page (except the Overview page) in the Unified CCE Administration interface and the online help specific to that page is displayed in a pop-over window. You can navigate to the previous or next page in the online help using the following keys:

- MAC - **Command + left arrow** or **Command + right arrow**
- Windows - **Alt+ right arrow** or **Alt + left arrow**

Lists

List Windows

Most tools open to a List window that has rows for all currently configured objects. For example, the Teams tool has a list with a row for each team, and the Call Types tool has a list with a row for each call type. List windows allow you to search, sort, edit, and delete from the list.

Permissions on List windows vary for administrators and supervisors and are noted in the topic for each tool.

Search a List

There is a Search field on the List window for most tools. The search interface is similar, with small variations, depending on the tool.

Search and Administrators

If you sign in as a global administrator, a search returns all objects.

If you sign in as a departmental administrator, a search returns all objects in the departments you administer, as well as all global objects (objects that are in no departments).

Basic Search

Some tools offer a basic search on the **Name** (or name-equivalent) and **Description** fields.

Enter all or part of either value to find matches. Clear the search by deleting text from the Search field.

Search for Tools with Department IDs

For objects that can be associated with a department, you can click the + icon to the right of the Search field to open a popup window, where you can:

- Enter a name or description (for call types and precision queues add **id**).
- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Departments is an OR search.)

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

Agent Advanced Search

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.
- Enter a username, agent ID, first or last name, or description to search for that string.
- Enter one or more team names separated by spaces. (Team is an OR search--the agent or supervisor must be a member of one of the teams.)
- Enter one or more attribute names separated by spaces. (Attributes is an AND search--the agent or supervisor must have all attributes.)
- Enter one or more skill group names separated by spaces. (Skill Groups is an AND search.)
- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

  Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Departments is an OR search.)

Related Topics

Departments, on page 119

Sort a List

If a column in a List window has an arrow icon in the column header, click the **arrow** to sort in ascending or descending order.

Add Objects

Click **New** in a List window to open an Add window where you can complete fields to create and save a new object.

Update Objects

To edit an object in a List window, click in the row for that object. This opens a window where you can make and save modifications. This table explains which fields are editable for each tool.

In the List window for the Agent tool, you can edit descriptions, desk settings, and teams for multiple agents at once (see Edit Description, Desk Settings, and Teams for Multiple Agents, on page 88).

In the List window of the Dialed Number tool, you can edit the ringtone media file for multiple Dialed Numbers at once (see Add and Update Ringtone Media File for Multiple Dialed Numbers, on page 183).

Remember Not all tools are available for all Deployment Types.

Tool	Editable Fields
Administrators	All fields
Agents	All fields except **Site** and **Peripheral Set**. If an agent is not enabled for single sign-on, you can check **Change Password** to reset the agent's password. **Note** • When you change the team association for an agent record in Packaged CCE, the same change is updated in the corresponding collection in Unified Intelligence Center. • When you change the username for a supervisor's record in Packaged CCE, the same is updated in the corresponding user account in Unified Intelligence Center. • For an existing supervisor's record, if you uncheck the **Is Supervisor** check box, the corresponding user account is deleted from Unified Intelligence Center.
Attributes	All fields except **Type**.
Bucket Intervals	**Name** You cannot edit the built-in bucket interval.
Bulk Jobs	No fields
Business Hours	**General** tab: All fields. **Regular Hours** tab: All fields. **Special Hours & Holidays** tab: All fields. **Status Reasons**: The **Status Reason** field is editable.
Call Types	All fields except the system-generated ID.
Campaigns	**General** tab: All fields except **Type** field. **Skill Group** tab: You can add and delete the Skill Groups using **Add** and **Delete** buttons. **Advanced** tab: All fields.

Tool	Editable Fields
Desk Settings	All fields
Dialed Numbers	All fields except **Site**, **Routing Type** , **Peripheral Set**and **Media Routing Domain**.
Expanded Call Variables	For user-defined array and scalar expanded call variables, **Name**, **Description**, **Maximum Length**, **Enabled**, and **Persistent** are editable. For built-in expanded call variables, **Enabled** and **Persistent** are the only editable fields.
Media Routing Domains	All fields You cannot edit the built-in Cisco_Voice MRD or Multichannel MRDs for Enterprise Chat and Email.
Network VRU Scripts	All fields
Precision Queues	All fields
Reason Labels	**Label**, **Description** , **Global** , and **Team Specific**
Roles	For custom roles, except for the **Administrators**, **Departments** and **Roles** fields in the **Access** category, all fields on both tabs are editable. You cannot edit the built-in roles.
Routing Pattern	All fields except **Routing Pattern**, **Site** and **Pattern Type**.
Location	All fields except **Location Name**.
SIP Server Group	All fields except **Domain Name FQDN**, **Site**, and **Type**.
Teams	All fields except **Site** and **Peripheral Set**. **Note** When you update an existing team record in Packaged CCE, the same changes are also updated in the corresponding collection in Unified Intelligence Center.
Skill Groups	All fields except **Site**, **Media Routing Domain** , **Peripheral Set** and **Peripheral Number**. **Note** The **Peripheral Number** field is generated automatically when you add and save a new skill group. It shows the number of the skill group, as known on the peripheral.

Delete Objects

To delete an object from a List window, hover over the row for that object to see the **x** icon at the end of the row. Click the **x** icon and confirm your intention to delete.

Departmental administrators cannot delete global objects. Objects are identified as global in the Department column in the List window.

When you delete an object from Unified CCE Administration, the system does one of the following:

- Immediately deletes the object.
- Marks the object for deletion and enables permanent deletion. (You delete the object permanently using the Deleted Objects tool in Configuration Manager.)
- Shows an error message explaining why the object cannot be deleted in its current state.

You cannot delete certain objects, including:

- Objects set as system defaults, such as the default desk settings.
- Objects referenced by other objects, such as a call type that is referenced by a dialed number.
- Most built-in objects, such as built-in expanded call variables.

This table lists the delete types for all Unified CCE Administration objects. Available objects depend on your role and deployment type.

Tool	Delete Type	Notes
Administrators	Permanent	—
Agents	Marked	**Note** When you delete an agent for which **Is Supervisor** check box is selected, the corresponding user account in Unified Intelligence Center is also deleted. When you delete an agent, the association with team is also removed and same is updated in the corresponding collection in Unified Intelligence Center.
Attributes	Marked	—
Bucket Intervals	Marked	—
Bulk Jobs	Permanent	Deletes the bulk job, its content file, and its log file from the host computer that created it. You can delete a bulk job that is in queue, has completed, or has failed. You cannot delete a bulk job that is in process. If your deployment includes two AW server hosts, you must delete a bulk job from the Unified CCE AW host on which it was created.

Tool	Delete Type	Notes
Business Hours	Permanent	You cannot delete a business hour associated with a script. You must first dissociate the business hour from the script.
Status Reasons	Permanent	—
Call Types	Marked	—
Campaigns	Marked	—
Desk Settings	Permanent	—
Dialed Numbers	Marked	—
SIP Server Group	Permanent	You cannot delete the SIP Server Group associated with a Routing Pattern. You must first remove the SIP Server Group from the Routing Pattern.
Expanded Call Variables	Marked	—
Media Routing Domains	Permanent	You cannot delete the built-in Cisco_Voice MRD or Multichannel MRDs for Enterprise Chat and Email (ECE).
Network VRU Scripts	Permanent	—
File Transfer Job	Permanent	Deletes the file transfer job, its job details file, and its log file from the host computer where it is created. You cannot delete a file transfer job that is in processing state.
Precision Queues	Marked	Depends on whether the precision queue is referenced statically or dynamically in a script. .
Reason Labels	Marked	—
Roles	Permanent	—
Routing Pattern	Permanent	—
Location	Permanent	—
Teams	Permanent	**Note** When you delete a team in Packaged CCE, the corresponding collection is also deleted in Unified Intelligence Center.
Skill Groups	Marked	—

Related Topics

Permanent Deletion

Popup Windows

Popup window selection

Many Add and Edit windows have popup windows for searching and choosing objects that are relevant to that tool.

Some popup windows allow you to chose one object. Other popup windows allow you to select multiple objects. For example, because an agent can be on only one team, the popup window for adding an agent to a team allows only one selection, while the Skill Group Members popup window allows you to select one or more agents to add to the skill group.

Click the + icon to open the popup window, where you can locate and select items that are configured.

Keyboard Shortcuts

Press the question mark (**?**) key to open a window that shows the keyboard shortcuts that are applicable for that tool and for your status (Supervisor or Administrator).

Tip The keyboard shortcuts window does not open when you press the (**?**) key in a text field. Press the **esc** key to remove focus from the text field and then press the (**?**) key.

System and Device Sync Alerts

Unified CCE Administration includes icons to notify users of any system alerts and device out-of-sync alert.

System Alerts

In Unified CCE Administration, you can monitor the status of the systems. The Alerts icon on the page includes alert count.

To view the alert and validation rule of a machine, click the Alerts icon. The Inventory page opens where you can view more details on the errors. For more information on server status rules, see Monitor Server Status Rules for Packaged CCE 2000 Agents Deployment

Device Out of Sync Alerts

In Unified CCE Administration, the configured data is synchronized with respective devices deployed in the inventory. If configured data synchronization fails with any device, the device is marked as out-of-sync and the Out of Sync device alert icon appears at the top of the page.

You can click the icon to open the Inventory page, and view data synchronization status of Cisco Unified Customer Voice Portal (CVP), Cisco Finesse Primary, Cisco Unified Intelligence Center (CUIC) Publisher, Enterprise Email and Chat (ECE) Web Server, and Cisco Virtualized Voice Browser (VVB).

You can perform manual synchronization of data on each In Sync and Out of Sync device in the Inventory. See Manual Synchronization of Configured Data, on page 10.

Manual Synchronization of Configured Data

This procedure explains how to manually synchronize configured data. You can do a Full Sync (for CVP) or a Differential sync.

Full Sync: This option is enabled for all CVPs (Main site and remote site) . Full Synchronization reinitializes the device (CVP redeploy) and synchronizes all configuration data from the time when the initial configuration was done. Use this option after you reimage or reinstall the CVP Server.

Differential Sync: This option synchronizes the configured data from the time the device was out of sync.

Procedure

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

Step 2 If the device Sync Status is **In Sync**, click the **Sync** icon and select **Full Sync**.

Step 3 If the device Sync Status is **Out of Sync**, click the **Sync** icon and select one of the following options

- **Differential Sync**
- **Full Sync**

Step 4 Click the **Sync** button.

Note If the Full Sync operation is successful, you must restart the CVP device.

Infrastructure Settings

Smart Licensing

Smart Licensing Overview

Cisco Smart Software Licensing is a flexible software licensing model that streamlines the way you activate and manage Cisco software licenses across your organization. Smart Licenses provide greater insight into software license ownership and consumption, so that you know what you own and how the licenses are being used. The solution allows you to easily track the status of your license and software usage trends. It pools the license entitlements in a single account and allows you to move licenses freely across virtual accounts. Smart Licensing is enabled across most of the Cisco products and managed by a direct cloud-based or mediated deployment model.

Smart Licensing registers the Product Instance, reports license usage, and obtains the necessary authorization from **Cisco Smart Software Manager (Cisco SSM)** or **Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)**.

You can use Smart Licensing to:

- View license usage and count.
- View the status of each license type and the product instance.

- View the product licenses available on Cisco SSM or Cisco SSM On-Prem.
- Register or deregister the Product Instance, renew license authorization and license registration.
- Sign in additional agents to Unified CCX up to the maximum limit that is configured in your OVA.

License Management

Smart Licensing can be managed by using Cisco SSM and License Management in Unified CCE Administration portal..

- **Cisco SSM—**Cisco SSM enables you to manage all your Cisco smart software licenses from a centralized website. With Cisco SSM, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances).

  You can access Cisco SSM from https://software.cisco.com, by clicking the Smart Software Licensing link under the License menu.

- **License Management in Unified CCE Administration portal—**Using the License Management option in the Unified CCE Administration portal, you can register or deregister the product instance, select your License Type, set transport settings or view the licensing consumption summary.

Prerequisites for Smart Licensing

The following are the prerequisites for configuring Smart Licensing:

- **Smart Licensing Enrollment**

  Set up Smart and Virtual accounts. For more information, see https://software.cisco.com/#module/SmartLicensing.

- **Adoption of License Integration Strategy**

  Decide how you want to connect your product instance to Smart Licensing servers:

  - **On-Cloud:** Configure Packaged CCE to connect to Cisco SSM On-Prem Cisco SSM.
  - **On-Premise:**

    1. Deploy the Cisco SSM On-Prem. For instructions on how to do this, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html.
    2. Configure Packaged CCE to connect to Cisco SSM On-Prem.

  For more information, see Smart License Deployments, on page 12.

- **Import the Rogger A certificate into the AW machines**

  1. Export Logger/Rogger A certificate and save it by using the url `https:<Logger/Roggerhostname>:443`
  2. Import the certificate in AW by using the following command:

     - `cd %CCE_JAVA_HOME%\bin`

     ```
     C:\Program Files (x86)\Java\jre1.8.0_221\bin>keytool.exe -keystore
     Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"
     -import -alias <alias name> -file <certicate with fully qualified path>
     ```

  3. Enter the truststore password when prompted.

4. Enter 'Yes' when prompted to trust the certificate.
5. Restart the Tomcat service.

Smart License Deployments

There are two software deployment options for Smart Licensing:

- Direct - Cisco Smart Software Manager (Cisco SSM)
- Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)

Direct - Cisco Smart Software Manager (Cisco SSM)

The Cisco SSM is a cloud-based service that handles your system licensing. The Product Instance can connect either directly to Cisco SSM or through a proxy server.

Cisco SSM allows you to:

- Create, manage, or view virtual accounts.
- Manage and track the licenses.
- Move licenses across the virtual accounts.
- Create and manage Product Instance Registration Tokens.

For more information about Cisco SSM, go to https://software.cisco.com.

Cisco Smart Software Manager On-Prem (Cisco SSM On-Prem)

Cisco SSM On-Prem is an on-premises component that can handle your licensing needs. When you choose this option, Packaged CCE registers and reports license consumption to the Cisco SSM On-Prem, which synchronizes its database regularly with Cisco SSM that is hosted on cisco.com.

You can use the Cisco SSM On-Prem in either Connected or Disconnected mode, depending on whether the Cisco SSM On-Prem can connect directly to cisco.com.

Configure Transport URL for Cisco SSM On-Prem with Smart Call-Home URL:
https://<OnpremCSSM>/Transportgateway/services/DeviceRequestHandler

Note The <OnpremCSSM> value must match with the SSM Tomcat Certificate Common Name or Subject Alternative Name. In the above URL, replace <OnpremCSSM> with FQDN or IP, based on the SSM Tomcat Certificate.

- **Connected**—Use when there is connectivity to cisco.com directly from the Cisco SSM On-Prem. Smart account synchronization occurs automatically.
- **Disconnected**—Use when there is no connectivity to cisco.com from the Cisco SSM On-Prem. Cisco SSM On-Prem must synchronize with Cisco SSM manually to reflect the latest license entitlements.

  For more information on Cisco SSM On-Prem, see https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html.

Evaluation Mode

After installation, Packaged CCE runs under the 90-day evaluation period. At the end of the evaluation period, if the system is not registered with Cisco SSM, it will enter a state of Enforcement where system operations are restricted. For more information, see *Enforcement Rules*.

Customers must Register the system with Cisco SSM or Cisco SSM On-Prem within 90 days. If the system is not registered before the end of the evaluation period, it will be moved to the Enforcement state where certain system functions are restricted.

Smart Licensing Task Flow

Complete these tasks to set up smart licensing for Packaged CCEUnified CVP.

Steps	Action	Description
Step 1	Create your Smart Account	Use the Smart Account to organize licenses according to your needs. To create a Smart Account, go to http://software.cisco.com After the Smart Account is created, Cisco SSM creates a default Virtual Account for this Smart Account. You can use the default account or create other Virtual Accounts.
Step 2	Obtain the Product Instance Registration Token	Generate a product instance registration token for your virtual account. For more information, see Obtain the Product Instance Registration Token.
Step 3	Configure Transport Settings for Smart Licensing	Configure the transport settings through which Packaged CCEUnified CVP connects to the Cisco SSM or Cisco SSM On-Prem. For more information, see Configure Transport Settings for Smart Licensing.
Step 4	Select the License Type	Select the License Type before registering the product instance. For more information, see Select License Type.
Step 5	Register with Cisco SSM	You can register Packaged CCEUnified CVP with Cisco SSM or Cisco SSM On-Prem. For more information, see Register with Cisco Smart Software Manager.

Note After performing the above steps, wait for 10-15 minutes for the correct status to get reflected in the UI. There is no need to restart the services.

Obtain the Product Instance Registration Token

Obtain the product instance registration token from Cisco SSM or Cisco SSM On-Prem to register the product instance. Generate the registration token with or without enabling the Export-Controlled functionality.

Note The **Allow export-controlled functionality on the products that are registered with this token** check box does not appear for Smart Accounts that are not permitted to use the Export-Controlled functionality.

Procedure

Step 1 Log in to your smart account in either Cisco SSM or Cisco SSM On-Prem.

Step 2 Navigate to the virtual account with which you want to associate the product instance.

Step 3 Generate the Product Instance Registration Token.

Note
- Select the **Allow export-controlled functionality on the products registered with this token** check box to turn on the Export-Controlled functionality for a product instance you want in this smart account. When you select this check box and accept the terms, you enable higher levels of encryption for products that are registered with this registration token. By default, this check box is selected.
- Use this option only if you are compliant with the Export-Controlled functionality.

Step 4 Copy the generated token. This token is required when registering Smart Licensing with Cisco SSM.

Configure Transport Settings for Smart Licensing

Configure the connection mode between Packaged CCEUnified CVP and Cisco SSM.

Note Configure the transport setting individually for all CVP devices installed in the deployment.

Procedure

Step 1 From Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management**.

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Note The system displays the following error if the CVP server you selected is not reachable or is not compatibile with your PCCE version.

```
The server is unreachable or is not on a version that supports this feature.
```

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

Step 3 Click **Transport Settings** to set the connection method.

Step 4 Select the connection method to Cisco SSM:

- **Direct**—Packaged CCEUnified CVP connects directly to Cisco SSM on cisco.com. This is the default option.
- **Transport Gateway**—Packaged CCEUnified CVP connects to Cisco SSM On-Prem for smart licensing. Enter the Cisco SSM On-Prem URL.
- **HTTP/HTTPS Proxy**—Packaged CCEUnified CVP connects to a proxy server, which connects to Cisco SSM. Enter the Fully Qualified Domain Name (FQDN) of the proxy server along with the port.

Step 5 Click **Save** to save the settings.

Select License Type

Smart Licensing offers two types of license—Flex and Perpetual and it also provides two different usage mode—Production and Non-Production.

- **Flex**—Flex license is a recurring subscription of Standard and Premium license. These subscriptions are renewed periodically, for example 1, 3, or 5 years.
- **Perpetual**—Perpetual license is a permanent and one-time payment license that offers Premium license.
- **Production**—Production mode is when the licenses are used on live systems to handle actual production traffic. Yes
- **Non-Production**—Non-production mode is used for labs, testing and/or staging areas, and not for live systems handling actual end-consumer traffic.

Select the License Type and Usage Mode corresponding to what you have purchased before registering the product instance.

Note If you select incorrect License Type, the product instance is placed in the Out-of-Compliance state. If this issue is unresolved, the product instance is placed in the Enforcement state where the system operations are impacted.

Procedure

Step 1 From Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management**.

Step 2 Click **License Type**.
The **Select License Type** page is displayed.

Step 3 Select the License Type and the Usage Mode corresponding to what you have purchased before registering the product instance.

Step 4 Select the License Type and the Usage Mode corresponding to what you have purchased before registering the product instance.

Step 5 Click **Save**.

Register with Cisco Smart Software Manager

The product instance has 90 days of evaluation period, within which, the registration must be completed. Else, the product instance gets into the enforcement state.

Register your product instance with Cisco SSM or Cisco SSM On-Prem to exit the Evaluation or Enforcement state.

Note After you register the product instance, you cannot change the license type. To change the license type, deregister the product instance.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Note The system displays the following error if the CVP server you selected is not reachable or is not compatible with your PCCE version.

```
The server is unreachable or is not on a version that supports this feature.
```

For details, see *Contact Center Enterprise Solution Compatibility Matrix*.

Step 3 Click **Register**.

Note
- Before you register the product instance, ensure to select the **License Type** and the communication mechanism in **Transport Settings**.

Step 4 In the **Smart Software Licensing Product Registration** dialog box, paste the product instance registration token that you generated from Cisco SSM or Cisco SSM On-Prem.

For information on generating the Registration Token, see the *Obtain the Product Instance Registration Token* section in Cisco Unified Contact Center Express Features Guide.

Step 5 Click **Register** to complete the registration process.

After registration, the **Smart Licensing Status** displays the following details.

Table 1: Smart Licensing Status

Smart License Status	Description
On Unsuccessful Registration	
Registration Status	Unregistered
License Authorization Status	Evaluation

Smart License Status	Description
Export-Controlled Functionality	Not Allowed
On Successful Registration	
Registration Status	Registered (Date and time of registration)
License Authorization Status	Authorized (Date and time of authorization)
Export-Controlled Functionality	Not Allowed
Smart Account	The name of the smart account
Virtual Account	The name of the virtual account
Product Instance Name	The name of the product instance
Serial Number	The serial number of the product instance

Entitlements are a set of privileges customers and partners receive when purchasing a Cisco service agreement. Using Smart Licensing, you can view the License consumption summary for the entitlements of different license types. The License consumption summary displays the License Name, Usage Count, and Status against each entitlement name.

You can update or purchase entitlements on the Cisco Commerce website. For more information, see https://apps.cisco.com/Commerce/.

Registration, Authorization, and Entitlement Status

Registration Status

This table explains the various productUnified CVP registration status for Smart Licensing in the Unified CCE Administration portal:

Table 2: Registration Status

Status	Description
Unregistered	Product is unregistered.
Registered	Product is registered. Registration is automatically renewed every six months.
Registration Expired	Product registration has expired because the ID Certificate issued by Cisco SSM is not renewed for more than 12 months.

Authorization Status

This table describes the possible productUnified CVP authorization status for Smart Licensing in the Unified CCE Administration portal:

Table 3: Authorization Status

Status	Description
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
Authorized	Product is in authorized or in compliance state. Authorization is renewed every 30 days.
Authorization Expired	Product authorization has expired. This usually happens when the product has not communicated with Cisco for 90 days. It is in an overage period for 90 days before enforcing restrictions.
Out-of-Compliance	Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.
Unauthorized	Product is unauthorized.
No License in Use	No Licenses are in use.

License Entitlement Status

This table describes the possible productUnified CVP instance license entitlement status for Smart Licensing in the Unified CCE Administration portal:

Table 4: License Entitlement Status

Status	Status Description
Authorization Expired	Product authorization has expired, when the product has not communicated with Cisco for 90 days.
Not Authorized	Product instance is not authorized.
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
In Compliance	Product is in authorized or in compliance state. Authorization is renewed every 30 days.
ReservedInCompliance	Entitlement is in compliance with the installed reservation authorization code.
Out-of-Compliance	Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.
Not Applicable	Entitlement is not applicable.
Invalid	Error condition state.
Invalid Tag	Entitlement tag is invalid.

Status	Status Description
No License in Use	Entitlement is not in use.
Waiting	Waiting for an entitlement request's response from Cisco SSM or Cisco SSM On-Prem.
Disabled	Product instance is deactivated or disabled.

Out-Of-Compliance and Enforcement Rules

Out-of-Compliance

The Product Instance reports license usage to Cisco SSM every 15 minutes. If your license consumption is more than the entitlements for four consecutive reporting intervals, the Product Instance is pushed to the Out-of-Compliance state. The Out-of-Compliance period is for 90 days, within which you need to purchase the additional licenses. If you fail to take corrective action within the 90 days period, the Product Instance is pushed to the Enforcement state.

All CVPs in a virtual account share the licenses from a pool. If the license consumption exceeds than those available in the pool, all CVPs in the virtual account follow the Out-of-Compliance and Enforcement rules.

Enforcement

The Product Instance is in the Enforcement state in the following scenarios:

- **Out-of-Compliance expiry**: When the Out-of-Compliance period of 90 days has expired.

  Purchase new licenses to exit the Enforcement state.

- **Authorization expiry**: When the Product Instance has not communicated with Cisco SSM or Cisco SSM On-Prem for 90 days and has not automatically renewed the entitlement authorizations.

  Renew the license authorizations to exit the authorization expiry state.

- **Evaluation expiry**: When the license evaluation period of 90 days has expired and the Product Instance is not registered with Cisco SSM.

  Register the Product Instance with Cisco SSM to exit the Evaluation expiry state.

Note In the Enforcement state, the following actions are blocked in CVP:

- Deploying application and updating application scripts in VXML server
- Deploying VXML applications REST call from the Unified CCE Administration interface

Notifications and Alerts

The system maintains real-time status of license usage after Product Instances are registered and activated. Administrators are notified through alerts, event logs, and emails on the status of licenses in the Smart and Virtual Accounts. Pay attention to system alerts and banners to get regular information on compliance status and take necessary action.

Following are some of the notification methods:

- Banner Notifications
- System Alerts

Banner Notifications

- The banner displays the aggregate license compliance status on the Unified CCE Administration portal. The banner is displayed only when any of the product instances in the deployment is in the Evaluation, Out-of-Compliance, or Enforcement state.

  The **License Compliance report** displays the license status of product instances in the deployment. The reporting hierarchy is Enforcement, Out-of-Compliance, and Evaluation. This means that if any of the product instances in the deployment is in the Enforcement state, the banner displays Enforcement state as the overall status. Click the **Learn More** option to view the consolidated **License Compliance report**.

- When licenses are consumed in a Non-Production System, a banner message, "You are using a Non-Production System", is displayed.

System Alerts

Smart Licensing related system alerts, which get auto-corrected, are displayed in Unified CCE Administration portal when:

- Smart License state is not initialized
- Smart Agent is not enabled
- Serial number is not generated

In the above conditions, a red system alert is displayed in the **Alerts** button on the Unified CCE Administration portal. The red circle against the name of the machine in the inventory indicates the identified issue and the immediate action needed. After the issue is resolved, a green circle against the name of the machine indicates the system is running fine, for example, when the Smart Agent is enabled or Smart License state is initialized.

Smart Licensing Tasks

After you successfully register Smart Licensing, you can perform the following tasks as per the requirement:

- **Renew Authorization**—The license authorization is renewed automatically every 30 days. Use this option to manually renew the authorization.
- **Renew Registration**—The initial registration is valid for one year. Registration is automatically renewed every six months. Use this option to manually renew the registration.
- **Reregister**—Use this option to forcefully register the product instance again.
- **Deregister**—Use this option to release all the licenses from the current virtual account.

Renew Authorization and Renew Registration are automated tasks that take place at regular intervals. If there is a failure in the automated process, you can manually renew authorization and registration.

For more information, see *Smart License Management* section in *Cisco Unified Contact Center Express Admin and Operations Guide*.

Note You have to Deregister and Reregister manually.

Renew Authorization

The license authorization is renewed automatically every 30 days. The authorization status expires after 90 days if the product is not connected to Cisco SSM or Cisco SSM On-Prem.

Use this procedure to manually renew the License Authorization Status for all the licenses listed in the License Type.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Note The system displays the following error if the CVP server you selected is not reachable or is not compatibile with your PCCE version.

```
The server is unreachable or is not on a version that supports this feature.
```

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

Step 3 Click **Action** > **Renew Authorization**.

This process takes a few seconds to renew the authorization and close the window.

Renew Registration

Use this procedure to manually renew your certificates.

The initial registration is valid for one year. Renewal of registration is automatically done every six months, provided the product is connected to Cisco SSM or Cisco SSM On-Prem.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management** .

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Note The system displays the following error if the CVP server you selected is not reachable or is not compatibile with your PCCE version.

```
The server is unreachable or is not on a version that supports this feature.
```

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

Step 3 Click **Action** > **Renew Registration**.

This process takes a few seconds to renew the authorization and close the window.

Reregister License

Use this procedure to reregister Packaged CCEUnified CVP with Cisco SSM or Cisco SSM On-Prem.

Note Product can migrate to a different virtual account when reregistering with the token from a new virtual account.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management.**

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Note The system displays the following error if the CVP server you selected is not reachable or is not compatibile with your PCCE version.

```
The server is unreachable or is not on a version that supports this feature.
```

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

Step 3 Click **Action** > **Reregister**.

Step 4 In the **Smart Software Licensing Product Registration** dialog box, paste the copied or saved Registration Token Key that you generated using the Cisco SSM or Cisco SSM On-Prem in the Product Instance Registration Token text box.

Step 5 Click **Reregister** to complete the reregistration process.

Step 6 Close the window.

Deregister License

Use this procedure to deregister Packaged CCEUnified CVP from Cisco SSM or Cisco SSM On-Prem and release all the licenses from the current virtual account. All license entitlements that are used for the product are released to the virtual account and is available for other product instances to use.

Note If Packaged CCEUnified CVP is unable to connect to Cisco SSM or Cisco SSM On-Prem, and the product is deregistered, then a confirmation message notifies you to remove the product manually from Cisco SSM or Cisco SSM On-Prem to free up licenses.

Note After deregistering, the product reverts to the Evaluation state if the evaluation period is not expired. All the license entitlements that are used for the product are immediately released to the virtual account and are available for other product instances to use them.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings** > **License Management** .

Step 2 The license information of the first CVP server in the **Device Name** drop-down list is displayed by default. From the **Device Name** drop-down list, select a CVP server.

Note The system displays the following error if the CVP server you selected is not reachable or is not compatibile with your PCCE version.

```
The server is unreachable or is not on a version that supports this feature.
```

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

Step 3 Click **Action** > **Deregister**.

Step 4 On the **Confirm Deregistration** dialog box, click **Yes** to deregister.

Smart Licensing Configurations

Unified CVP Release12.5 uses the following configuration files for Smart Licensing operations.

- C:\Cisco\CVP\conf\smartlicense.properties
- C:\Cisco\CVP\conf\licensetype.properties
- C:\Cisco\CVP\conf\Entitlementmapper.csv

Note Do not edit, delete, or access these files without contacting Cisco TAC. Any change to these files can cause operational impact.

Handling SocketTimeoutException:

If there is a delay in communication between the OMAP and CVP servers, and the **SocketTimeoutException** error is seen in the Catalina log, perform the following steps:

1. In the OAMP server, navigate to the following location:
   `%CVP_HOME%\OPSConsoleServer\Tomcat\webapps\ROOT\WEB-INF\classes`
2. Open the file shindig.properties and edit as follows:
   a. Change `shindig.http.client.connection-timeout-ms=5000` to `shindig.http.client.connection-timeout-ms=10000`.
   b. Add the read-timeout configuration after the connection-timeout configuration:
      `shindig.http.client.read-timeout-ms=100000`
3. Save the shindig.properties file.
4. Restart the CVP OPS Console service and login to OAMP again.

Manage Devices

You can configure any of the following components:

- CVP Server
- CVP Reporting Server
- VVB
- Finesse
- Single Sign-on Setup

The term *device* refers to a configurable application or platform. More than one device can reside on a server. For example, one physical server can contain a CVP Server and a Reporting Server. In this case, each device is configured with the same IP address.

CVP Server Services Setup

As part of Packaged CCE fresh install, the CVP Server is added with default configuration values. You can configure:

- ICM Service
- SIP Service
- IVR Service
- VXML Server
- Infrastructure

Important Except for the configurations that require a Call Server restart, configure all the other CVP Server configurations during off-peak hours (not during heavy call load).

For shutting down services of call server/reporting server, see Graceful Shutdown of Call Server or Reporting Server.

Set Up ICM Service

The ICM Service enables communication between Unified CVP components and the ICM Server. It sends and receives messages on behalf of the SIP Service, the IVR Service, and the VXML Service. You install the ICM Service with the CVP Server.

You must configure the ICM Service if you add or edit a CVP Server and use any of these call flow models:

- Call Director
- VRU-Only
- Comprehensive

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Server**.

Step 2 Choose the site name for the ICM Service. By default, it is Main.

Step 3 Complete the following fields:

Table 5: ICM Service Configuration Settings

Field	Required?	Description
VRU Connection Port	yes	The port number on which the ICM Service 5000 listens for a TCP connection from the ICM PIM. Default is 5000.
Maximum Length of DNIS	yes	The maximum length of an incoming Dialed Number Identification Service (DNIS). Range is 1 - 99999 characters. Look for this information in your network dial plan. For example, if the gateway dial pattern is 1800******, the value of Maximum Length of DNIS must be 10. The number of DNIS digits from the PSTN must be less than or equal to the maximum length of the DNIS field. **Note** If you use the Correlation ID method in your ICM script to transfer calls to Unified CVP, the maximum length of DNIS must be the length of the label that is returned from the ICM for the VRU leg of the call. When the ICM transfers the call, the Correlation ID is appended to the label. Unified CVP then separates the two, assuming that any digits greater than the maximum length of DNIS are the Correlation ID. The Correlation ID and the label are then passed to the ICM.
Enable secure communication with VRU PIM	-	Enables secure communication between ICM and the Unified CVP Server.

Field	Required?	Description
Trunk Utilization		
Enable Gateway Trunk Reporting	-	Enables the gateway trunk reporting.
Maximum Gateway Ports	no	The value used for setting the maximum number of ports that a gateway supports in a CVP deployment. This is used to calculate the number of ports to report to the Unified ICM Server for each gateway. Default is 700.
Monitored Gateways	no	The list of gateways available for trunk reporting. Click + (Add) to add a new gateway.

Step 4 Click **Save**.

Set Up IVR Service

You must configure the IVR Service if you add a new Unified CVP Server or edit a Unified CVP Server in any of these call flow models:

- Call Director, using SIP protocol
- VRU-Only
- Comprehensive, using SIP protocol

The IVR Service creates VXML documents that implement the Micro-Applications based on Run Script instructions received by the ICM. The VXML pages are sent to the VXML Gateway to be run. The IVR Service can also generate external VXML through the Micro-Applications to engage the Unified CVP VXML Server to generate the VXML documents.

The IVR Service plays a significant role in implementing a failover mechanism: those capabilities that can be achieved without ASR/TTS Servers, and VXML Servers. Up to two of each such servers are supported, and the IVR Service orchestrates retries and failover between them.

Before you begin

Configure the following servers before setting up the IVR Service:

- ICM Server
- Media Server
- ASR/TTS Server
- Unified CVP VXML Server
- Gateway

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Server**.

Step 2 Click the **IVR** tab. Complete the following fields:

Table 6: IVR Service Configuration Settings

Field	Required?	Description
Use Security for Media Fetches	-	If you select **No** (default), the HTTP URLs are generated to the Media Servers. **Note** The default setting is only applicable if the client is SIP Service and the Media Server is not set to a URL that explicitly specifies an HTTP/HTTPS scheme. Select **Yes** to generate the HTTPS URLs to the Media Servers.
Use Backup Media/VXML Servers	-	If you select **Yes** (default) and a Media Server is unavailable, the gateway attempts to connect to the backup Media Server.
Use Host Names for Default Media/VXML Servers	-	By default, the IP address is used for the VXML Server and the Media Server. If you enables this field, the hostnames are used rather than the IP addresses. **Note** When you enable this field, enable the High Availability(HA) for Media Server in each CVP Server in the site after you save the configuration. To enable HA for Media Server, open the mediaServer.properties file in the C:\Cisco\CVP\conf folder and configure the following: • MediaServer.1.hostName = <Media Server Host> • MediaServer.1.ip = <Media Server IP> The IP and hostname must match the default media server IP and hostname in the Unified CCE Administration. Define the corresponding <hostname>-backup entry to backup Media Server IP in VXML Gateway and Virtualized Voice Browser(VVB). When the primary host name fails, the media files fetch request can be served from backup media server.

Field	Required?	Description
Call Timeout	yes	The number of seconds the IVR Service waits for a response from the SIP Service before timing out. This setting must be longer than the longest prompt, transfer, or digit collection at a Voice Browser. If the timeout is reached, the call is canceled but no other calls are affected. The only downside to making the number arbitrarily large is that if calls are being stranded, they are not removed from the IVR Service until this timeout is reached. Minimum is 6 seconds. Default is 7200 seconds.
Default Media Server	no	From the **Default Media Server** drop-down list, choose the default media server.

Step 3 Click **Save**.

Set Up SIP Service

You must set up the SIP Service if you add a new CVP Server in of these call flow models:

- Call Director
- Comprehensive

Session Initiation Protocol (SIP), RFC 3261, is the primary call control protocol in Unified CVP. The SIP Service uses SIP to communicate with other Unified CVP solution components, such as the SIP Proxy Server, the VXML and Ingress Gateways, and Cisco Unified Communications Manager SIP trunks and SIP phones.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Server**.

Step 2 Click the **SIP** tab. Complete the following fields:

Table 7: SIP Service Settings

Field	Required?	Description
Enable Outbound Proxy	-	Select **Yes** to use a Cisco Unified SIP proxy server. Default is No.
Outbound Proxy Host	no	Select **Enable Outbound Proxy** to view the **Outbound Proxy Host** drop-down list. It displays a list of external SIP Server Groups.
Outbound Proxy Port	no	Default is 5060.
DNS SRV		

Field	Required?	Description
Enable DNS SRV Type Query	-	Select **Yes** to use DNS SRV for outbound proxy lookup. **Note** If you enable Resolve SRV records locally, you must select **Yes** to ensure the feature works properly.
Resolve DNS SRV Locally	-	Select to resolve the SRV domain name with a local configuration file instead of a DNS Server. **Note** If you enable Resolve SRV records locally, you must select **Yes** to use the DNS SRV type query. Otherwise, this feature will not work.
Outgoing Transport Type	no	Specifies the outgoing transport. You can set it to TCP or UDP. Default is TCP.
Port Number for Incoming SIP Requests	yes	Specifies the port to be used for incoming SIP requests. Default is 5060.
Prepend Digits	no	Specifies the number of digits to be removed for SIP URI user number. Default is 0.
Use Error Refer	no	Flags for play error tone when a call fails to caller. Default is False.
SIP Info Tone Duration	yes	Specifies the wait time in milliseconds for the SIP info tone. It is an optional value for the list addition. Default is 100.
SIP Info Comma Duration	yes	Specifies the wait time in milliseconds for the SIP info comma. It is an optional value for the list addition. Default is 100.
SIP Header Passing to ICM		
Header Name	no	Specifies the SIP header name. Click + (Add) to add a new SIP header to be passed to ICM. It can support up to 255 characters.
Parameter	no	This field is optional for list addition. It can support up to 255 characters.
Security Properties		
Incoming Secure Port	no	Specifies the port to be used. Default is 5061.

Field	Required?	Description
Supported TLS Version	yes	Allows you to select the TLS versions supported for securing the SIP signaling on the IVR leg. The TLS versions currently supported are TLSv1.0, TLSv1.1, and TLSv1.2. Default is TLSv1.2. **Note** When you select a given TLS version, Unified CVP supports the SIP TLS requests for that version and the higher supported versions.
Supported Ciphers	no	This field defines the ciphers, which is supported by Unified CVP, with key size lesser than or equal to 2048 bits. The default cipher is TLS_RSA_WITH_AES_128_CBC_SHA, which is prepopulated and cannot be deleted as it is mandatory for TLSv1.2. Cipher configuration is available only if TLS is enabled. Click + (Add) to add a new cipher.

Note After you add the required ciphers restart the system for more information, refer to the topic *Generate CVP ECDSA Certificate with OpenSSL* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html

Note The dialed number uses default values to play the ringtone and the error tone. These values cannot be edited.

Step 3 Click **Save**.

Set Up VXML Server

From the Unified CVP VXML Server Configuration tab, you can enable the reporting of Unified CVP VXML Server and call activities to the Reporting Server. When enabled, the Unified CVP VXML Server reports on the call and the application session summary data. The call summary data includes call identifier, start and end timestamp of calls, ANI, and DNIS. The application session data includes application names, session ID, and session timestamps.

If you choose detailed reporting, the Unified CVP VXML Server application details are reported, including element access history, activities within the element, the element variables, and the element exit state. Customized values added in the **Add to Log** element configuration area in Call Studio applications are also included in reporting data. You can also create report filters that define the data to be included and excluded from being reported.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Server**.

Step 2 Click the **VXML Server** tab. Complete the following fields:

Table 8: VXML Server Configuration Properties

Field	Required?	Description
Enable Reporting for this Unified CVP VXML Server	-	Indicates if the Unified CVP VXML Server sends data to the Reporting Server. If disabled, no data is sent to the Reporting Server, and reports do not contain any VXML application data.
Enable Reporting for VXML Application Details	-	Indicates whether VXML application details are reported.
VXML Applications Details: Filters		
Inclusive Filters	no	Lists applications, element types, element names, element fields, and ECC variables to include in the reporting data. A semicolon-separated list of text strings. A wildcard character (*) is allowed within each element in the list.
Exclusive Filters	no	Lists applications, element types, element names, element fields, and ECC variables to exclude from the reporting data.

Step 3 Click **Save**.

Set Up Infrastructure

The CVP Server provides SIP, IVR, and ICM call services. The CVP Reporting Server provides reporting services. Changes to the infrastructure settings affect all services that use threads, publish statistics, send syslog events, or perform logging and tracing. For example, changing the syslog server setting applies to all services that write to syslog.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Server**.

Step 2 Click the **Infrastructure** tab. Complete the following fields:

Table 9: Infrastructure Service Configuration Settings

Field	Required?	Description
Log File Properties		
Max Log File Size	yes	The maximum size of a log file in megabytes before a new log file is created. Range is 1 - 100MB. Default is 10MB.

Field	Required?	Description
Max Log Directory Size	yes	The maximum size of a directory to allocate disk storage for log files. Range is 500 - 500000MB. Default is 20000MB. **Note** Modifying the value to a setting that is below the default value might cause logs to be quickly rolled over. Consequently, the log entries might be lost, which can affect troubleshooting. The log folder size divided by the log file size must be less than 5000.
Configuration: Primary Syslog Server Settings		
Primary Syslog Server	no	The hostname or the IP address of the primary syslog server to send the syslog events from a CVP application.
Primary Syslog Server Port Number	no	The port number of the primary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Primary Backup Syslog Server	no	The hostname or the IP address of the primary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.
Primary Backup Syslog Server Port Number	no	The port number of the primary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Configuration: Secondary Syslog Server Settings		
Secondary Syslog Server	no	The hostname or the IP address of the secondary syslog server to send the syslog events from a CVP application.
Secondary Syslog Server Port Number	no	The port number of the secondary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Secondary Backup Syslog Server	no	The hostname or the IP address of the secondary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.
Secondary Backup Syslog Server Port Number	no	The port number of the secondary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.

Step 3 Click **Save**.

Unified CVP Security

Secure GED 125 Communication between Call Server and ICM

You can secure GED 125 communication by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Note By default, mutual authentication between ICM and Call Server is enabled. To disable mutual authentication, go to `%CVP_HOME%\conf\icm.properties` and set the **ICM.Secure.UseClientAuth** property to *FALSE* and restart the Call Server.

Before you begin:

For generating ECDSA certificates in ICM, refer to the *How to enable ECDSA for Unified CCE core components* section in the *Security Guide for Cisco Unified ICM/Contact Center Enterprise, Release 12.6(1)* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Self-Signed Certificates

Generate Certificate on CVP Call Server

Procedure

Step 1 http://acrsrv-app-prd-01:8080/Export the Call Server certificate by running.**%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias callserver_certificate -file %CVP_HOME%\conf\security\<callserver_certificate>**

Step 2 Enter the keystore password when prompted.

Step 3 Restart the Call Server service to load the new certificates.

Import Certificate into ICM

Procedure

Step 1 Copy the self-signed CVP Call Server certificate downloaded from CVP to the ICM box (PG).

Step 2 Open the command prompt and go to `c:\icm\bin`.

Step 3 Type **CiscoCertUtil.exe /install <callserver_certificate>**.
This imports the certificate to the Trusted Root Certification Authorities.

Note Repeat the procedure for multiple PIMs and for Side A and Side B.

Generate Certificate on ICM Server

Before you begin

If there is an existing host.pem certificate in `c:\icm\ssl\certs`, then skip the following procedure and go to the Section, On Call Server.

Procedure

Step 1 Log into the ICM (PG) box. Go to the command prompt and type **CiscoCertUtil.exe /generatecert**.

```
C:\icm\bin>ciscocertutil.exe /generatecert
SSL config path = C:\icm\ssl\cfg\openssl.cfg
SYSTEM command is C:\icm\ssl\bin\openssl.exe req -x509 -newkey rsa:2048 -days 7300 -nodes
-subj /CN=PG-SIDEA.pcce.com -out
C:\icm\ssl\certs\host.pem -keyout C:\icm\ssl\keys\host.key
Generating a 2048 bit RSA private key
...................
....
writing new private key to 'C:\icm\ssl\keys\host.key
..........
Certificate path: C:\icm\ssl\certs\host.pem , Key path: C:\icm\ssl\keys\host.key
```

The client certificate and key are generated and stored as host.csr and host.key in `C:\icm\ssl\certs` folder.

Step 2 Cycle VRU PG.

Import ICM Certificate into CVP Call Server

Procedure

Step 1 Log into the CVP Call Server box. Create a folder and copy host.pem to `c:\IcmCertificate`.

Step 2 From the command prompt, run **%CVP_HOME%\jre\bin\keytool.exe -import -v -alias icm_certificate -storetype JCEKS -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -file c:\IcmCertificate\host.pem**.

Step 3 Enter the keystore password when prompted. Click **Yes**.

Step 4 Restart the Callserver service to load the new certificates.

Note Repeat the procedure if you have multiple Call Servers.

CA Certificates

Generate CA Certificate on CVP Call Server

Log in to the Call Server. Retrieve the keystore password from the *security.properties* file.

Note At the command prompt, enter **more %CVP_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

Procedure

Step 1 Remove the existing certificate by running the following command:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias callserver_certificate

Step 2 Enter the keystore password when prompted.

Step 3 Generate a new key pair for the alias with the selected key size by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias callserver_certificate -v -keysize 2048 -keyalg RSA**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
 [Unknown]: <Specify the FQDN of the CVP server. Example: cisco-cvp-211@example.com >
What is the name of your organizational unit?
 [Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
 [Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
 [Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
 [Unknown]: <specify the name of the state/province>  E.g. KAR
What is the two-letter country code for this unit?
 [Unknown]: <specify two-letter Country code>  E.g. IN

Specify 'yes' for the inputs.
```

Step 4 Generate the CSR certificate for the alias by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias callserver_certificate -file %CVP_HOME%\conf\security\callserver.csr** and save it to a file (for example, callserver.csr).

Step 5 Enter the keystore password when prompted.

Step 6 Download the callserver.csr from `%CVP_HOME%\conf\security\` and sign it from CA.

Step 7 Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`.

Step 8 Install the root CA certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>**.

Step 9 Enter the keystore password when prompted.

Step 10 Install the signed certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias callserver_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>**.

Import Root CA Certificate into ICM

Procedure

Step 1 Copy the root CA certificate to the ICM (PG) box.

Step 2 Open the command prompt and go to `c:\cisco\icm\bin`.

Step 3 Type **CiscoCertUtil.exe /install rootCA.pem**.
This imports the certificate to the Trusted Root Certification Authorities.

Generate CA Certificate on ICM

Procedure

Step 1 Navigate to `C:\icm\ssl\keys` and remove the old 'host.key'(if available).

Step 2 Log into the ICM (PG) box. Go to the command prompt and type **CiscoCertUtil.exe /generateCSR**.

```
C:\icm\bin>CiscoCertUtil.exe /generateCSR
SSL config path = C:\icm\ssl\cfg\openssl.cfg
SYSTEM command is C:\icm\ssl\bin\openssl.exe req -new -key C:\icm\ssl\keys\host.key -out
C:\icm\ssl\certs\host.csr

Generating a 2048 bit RSA private key
..........................
.......
writing new private key to 'C:\icm\ssl\keys\host.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:KA
Locality Name (eg, city) []:BLR
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cisco
Organizational Unit Name (eg, section) []:ccbu
Common Name (e.g. server FQDN or YOUR name) []:abc.com
Email Address []:radmohan@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:*****
An optional company name []:cisco
```

The client certificate and key are generated and stored as host.csr and host.key in `C:\icm\ssl\certs` and `C:\icm\ssl\keys` folders respectively.

Step 3 Sign it from a CA. Follow the procedure Import Root CA Certificate into ICM, on page 36.

Note
- Remove the existing host.pem (if any) from `C:\icm\ssl\certs`.
- Save host.cer (CA-signed) as host.pem in `C:\icm\ssl\certs`.

Step 4 From the command prompt, run **C:\icm\bin>CiscoCertUtil.exe /install c:\icm\ssl\certs\host.pem**.

Step 5 Cycle VRU PG.

Secure SIP Communication between Call Server and Cisco VVB

You can secure SIP communication by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificates

On Call Server

Log in to the Call Server, retrieve the keystore password from the *security.properties* file.

Note At the command prompt, enter **more %CVP_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

Procedure

Step 1 Export the Call Server certificate by running **%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias callserver_certificate -file %CVP_HOME%\conf\security\<callserver_certificate.cer>**.

Step 2 Enter the keystore password when prompted.

Step 3 Copy the VVB/VXML gateway self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserver keystore by running **%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias vb_cert -file %CVP_HOME%\conf\security\<vvb certificate>**.

Note See Step 5 of the *On Cisco VVB* section to download a VVB certificate.

Step 4 Enter the keystore password when prompted.
A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.

Step 5 Use the list flag to check your keystore entries by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list**.

On Cisco VVB

Procedure

Step 1	Copy the CVP CallServer self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.
Step 2	Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain**.
Step 3	In **Certificate Purpose**, select **tomcat-trust**.
Step 4	Select the self-signed certificate of the Call Server and click **Upload**.
Step 5	Download the self-signed certificate of the VVB.
Step 6	Go to **OS Admin** > **Security** > **Certificate Management**.
Step 7	In the **Certificate** column, find the certificate named **tomcat**.
Step 8	Select the self-signed tomcat certificate and click **Download** .
Step 9	After the new certificate is uploaded, restart the node(s) using the CLI command **utils system restart**.
Step 10	Go to **Cisco VVB Administration** > **System Parameters** > **TLS**.
Step 11	Check TLS as **Enable**.
Step 12	Select the supported TLS version and click **Update**.
Step 13	Restart Cisco VVB Engine from the **VVB Serviceability** page.

CA-Signed Certificate

On Call Server

Log in to the Call Server. Retrieve the keystore password from the *security.properties* file.

Note At the command prompt, enter **more %CVP_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

On Cisco VVB

Procedure

Step 1	To generate the CSR certificate on VVB, open the administration page. From the **Navigation** drop-down list, choose **Cisco Unified OS Administration** and click **Go**.
Step 2	Go to **Security** > **Certificate Management** > **Generate CSR Generate Certificate signing Request**. Create the CSR against tomcat with the key-length as 2048.
Step 3	To download the generated CSR, click **Download CSR**. After the **Generate Certificate signing Request** dialog opens, click **Download CSR**.
Step 4	Open the certificate in Notepad, copy the contents and sign the certificate with CA.
Step 5	Upload the root certificate generated from the CA into VVB against tomcat-trust: a) Go to **Security** > **Certificate Management** > **Generate CSR** > **Upload certificate/certificate chain**. b) Choose **tomcat-trust** from the drop-down list.

c) Click **Browse** and select the certificate.
d) Click **Upload** to upload the root certificate of the Certificate Authority.

Step 6 Upload the signed certificate into VVB against tomcat.
a) Go to **Security** > **Certificate Management** > **Upload certificate/certificate chain**.
b) Choose **tomcat** from the drop-down list.
c) Click **Browse** and select the certificate.
d) Click **Upload**.

After the certificate is uploaded successfully, VVB displays the certificate signed by <CA hostname>.

Step 7 Restart the Tomcat service and the VVB engine.

For the configuration steps, see the *Manage System Parameters* section.

Secure HTTP Communication between VXML Server and Cisco VVB

You can secure HTTP communication by:

- Exchanging the self-signed certificates between the VXML Server and VVB or VXML Gateway.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

On VXML Server

Log in to the VXML Server. Retrieve the keystore password from the *security.properties* file.

Note At the command prompt, enter **more %CVP_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password wherever it prompts.

Procedure

Step 1 Export the VXML SERVER certificate by running **%CVP_HOME%\jre\bin\keytool.exe -export -v -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias vxml_certificate -file %CVP_HOME%\conf\security\<vxml_certificate.cer>**.

Step 2 Enter the keystore password when prompted.

Step 3 Copy the VVB/VXML gateway self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserver keystore by running **keystore.%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias vb_cert -file %CVP_HOME%\conf\security\<vvb certificate>**.

Note See Step 5 of the following Section, *On Cisco VVB* to download a VVB certificate.

Step 4 Enter the keystore password when prompted.
A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.

Step 5 Use the list flag to check your keystore entries by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list**.

On Cisco VVB

Procedure

Step 1 Copy the VXML Server self-signed certificate downloaded from CVP and upload it to VVB against tomcat-trust.

Step 2 Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain**.

Step 3 In **Certificate Purpose**, select **tomcat-trust**.

Step 4 Select the self-signed certificate of the VXML Server and click **Upload**.

Step 5 Download the self-signed certificate of the VVB.

Step 6 Go to **OS Admin** > **Security** > **Certificate Management**.

Step 7 In the **Certificate** column, select the **tomcat** certificate.

Step 8 Select the tomcat certificate and click **Download** .

Step 9 After the new certificate uploads, restart the Cisco Tomcat service.

Step 10 Go to **Cisco VVB Administration** > **System Parameters** > **TLS**.

Step 11 Check the **TLS** check box as **Enable**.

Step 12 Select the supported TLS version and click **Update**.

Step 13 Restart the Cisco VVB Engine from the **VVB Serviceability** page.

Note To enable secured connection in Application Management from the Cisco VVB UI, see *Cisco Virtualized Voice Browser Administration and Configuration Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/virtualized-voice-browser/tsd-products-support-series-home.html.

CA-Signed Certificate

On VXML Server

Log in to the VXML Server. Retrieve the keystore password from the *security.properties* file.

Note At the command prompt, enter **more %CVP_HOME%\conf\security.properties**.

Security.keystorePW = <Returns the keystore password>

Enter the keystore password when prompted.

Procedure

Step 1 Remove the existing certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -delete -alias vxml_certificate**.

Step 2 Generate a new key pair for the alias with selected key size by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias vxml_certificate -v -keysize 2048 -keyalg RSA**.

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
 [Unknown]: <specify the CVP host name appended with "VXML_Server"> E.g
cisco-cvp-211_VXML_Server
What is the name of your organizational unit?
 [Unknown]: <specify OU> E.g. CCBU
What is the name of your organization?
 [Unknown]: <specify the name of the org> E.g. CISCO
What is the name of your City or Locality?
 [Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
 [Unknown]: <specify the name of the state/province>  E.g. KAR
What is the two-letter country code for this unit?
 [Unknown]: <specify two-letter Country code>  E.g. IN
Specify 'yes' for the inputs.
```

Step 3 Generate the CSR certificate for the alias by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias vxml_certificate -file %CVP_HOME%\conf\security\vxmlserver.csr** and save it to a file .

Step 4 Enter the keystore password when prompted.

Step 5 Download the vxmserver.csr from `CVP %CVP_HOME%\conf\security\` and sign it from CA.

Step 6 Copy the root CA certificate and the CA-signed certificate to `%CVP_HOME%\conf\security\`

Step 7 Install the root CA certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>**.

Step 8 Enter the keystore password when prompted.

Step 9 Install the signed certificate by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias vxml_certificate -file %CVP_HOME%\conf\security\<filename_of_CA_signed_cert>**.

Step 10 Enter the keystore password when prompted.

Step 11 Restart the VXML Server.

On Cisco VVB

Procedure

Step 1 Upload the root certificate generated from the CA into VVB against tomcat-trust. Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain**, select **tomcat-trust** and upload the root certificate of the Certificate Authority.

Note If you use the same root certificate that was used in the Call Server configuration as described in Section, Secure Communication between Call Server and Cisco VVB and the certificate is already imported, then you can skip this step.

Step 2 Generate the CSR against tomcat with the key-length as 2048.

Step 3 Open the certificate in Notepad. Copy the contents and sign the certificate with CA.

Step 4 Restart the Tomcat service and the VVB engine.

To enable secure communications on the VXML Server, see Unified CVP VXML Server Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

To enable secure communications on the VXML Server (standalone), see Unified CVP VXML Server (Standalone) Setup *Administration Guide for Cisco Unified Customer Voice Portal* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-user-guide-list.html.

Secure HTTPS Communication between Media Server and Cisco VVB

This section describes how to import certificate from IIS MediaServer to Cisco VVB and how to import IIS CA-signed certificate.

Procedure

Step 1 Enter **https://<mediaserver>:443/** in the address bar of the web browser.

Step 2 In the **Security Alert** dialog box, click **View Certificate**.

Step 3 Click the **Details** tab

Step 4 Click **Copy to File**.

Step 5 In the **Certificate Export Wizard** dialog box, click **Base-64 encoded X.509 (.CER)**, and then click **Next**.

Step 6 In the **File to the Export** dialog box, specify a file name, and then click **Next**.

Step 7 Click **Finish**.
A message indicates that the export was successful.

Step 8 Click **OK** and close the **Security Alert** dialog box.

Step 9 Copy the CVP MediaServer self-signed certificate downloaded from the CVP and upload into VVB against **tomcat-trust**.

Step 10 Go to **OS Admin** > **Security** > **Certificate Management** > **Upload certificate/certificate chain** > **In Certificate Purpose*** select **tomcat-trust**, choose the self-signed certificate of the Call Server and press **Upload** button.

Step 11 Restart Cisco VVB Engine.

Secure Communication on CUCM

You can secure communication on CUCM by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

Procedure

Step 1 Log in to the CUCM OS Administration page.

Step 2 Go to **Security** > **Certificate Management**.

Step 3 Click **Generate Self-signed**.

Step 4 On the pop-up window, click **Generate** button.

Step 5 Restart Tomcat from CUCM CLI by running **utils service restart Cisco Tomcat**.

Note Tomcat will take a few minutes to stop and then start. If you access the CUCM UI during this time, you may receive a 404 error.

Step 6 When the CUCM UI is available, open the CUCM OS Administration page.

Step 7 Go to **Security** > **Certificate Management**.

Step 8 Click **Find** and identify the Self-signed certificate generated by the system.

Step 9 Click the CallManager Certificate name.

Step 10 In the dialog box, click **Download**.

CA-Signed Certificate

To configure TLS and SRTP, see *Security Guide for Cisco Unified Communications Manager 11.6* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Procedure

Step 1 Enter the following command in the CLI to set the CUCM in the mixed mode, and to register the endpoints in the encrypted mode:

```
admin: utils ctl set-cluster mixed-mode

This operation will set the cluster to Mixed mode.  Auto-registration is enabled on at least
 one CM node. Do you want to continue? (y/n):y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
You must reset all phones to ensure they received the updated CTL file.
You must restart Cisco CTIManager services on all the nodes in the cluster that have the
service activated.
admin:
```

Step 2 Choose **CUCM Admin Page** > **System** > **Enterprise Parameters**. Check if **Cluster Security Mode** is set to 1.

Step 3 Set the minimum TLS version command from the CLI:

```
admin:set tls client min-version 1.2

**WARNING** If you are lowering the TLS version it can lead to security issues **WARNING**

Do you really want to continue (yes/no)?y
Run this command in the other nodes of the cluster.
```

```
Restart the system using the command 'utils system restart' for the changes to take effect

Command successful
admin:set tls ser
admin:set tls server mi
admin:set tls server min-version?
Syntax:
set tls server min-version

admin:set tls server min-version 1.2

**WARNING** If you are lowering the TLS version it can lead to security issues **WARNING**

Do you really want to continue (yes/no)?y
Run this command in the other nodes of the cluster.

Restart the system using the command 'utils system restart' for the changes to take effect

Command successful
admin:
```

Step 4 Create an encrypted phone profile and the SIP trunk profile. Associate them with the phone and CUCM SIP trunk.

Step 5 Go to **System** > **Security** > **SIP Trunk Security Profile** and create a new SIP trunk security profile.

Step 6 On CUCM SIP Trunk, check the **SRTP Allowed** check box.

Step 7 From **SIP Trunk Security Profile** drop-down list, choose **TLS Secure Profile**.

Step 8 Restart the TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.

Step 9 Upload the root certificate generated from the CA to CUCM against CUCM-trust.

Step 10 Generate the CSR against CallManager and select the key-length as 2048.

Step 11 Sign the certificate on a CA https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/118731-configure-san-00.html.

Step 12 Click **Upload Certificate** on CUCM by selecting the certificate name as **CallManager**.

On successful completion, CUCM displays the description as *Certificate signed by <CA hostname>*.

Step 13 Restart TFTP and Cisco CallManager services on all the nodes in the cluster that run these services.

Secure Communication between Ingress Gateway and Call Server

You can secure communication between the Ingress Gateway and the Call Server by:

- Exchanging the self-signed certificates.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

To secure SIP connection between Cisco Ingress Gateway and Call Server, import the Call Server certificate on the IOS device during the device configuration.

Procedure

Step 1 Open the certificate that was exported in Step 1, on page 37.

Step 2 Click **View Certificate**.

Step 3 Click the **Details** tab.

Step 4 Click **Copy to File**.
The **Certificate ExportWizard** window appears.

Step 5 Click **Base-64 encoded X.509 (.CER)**, and then click **Next**.

Step 6 Specify a file name in the **File to the Export** dialog box, and then click **Next**.

Step 7 Click **Finish**. A message indicates that the export was successful.

Step 8 Click **OK** and close the **Security Alert** dialog box.

Step 9 Open the certificate in Notepad.

Step 10 Access the IOS ingress GW in the privileged EXEC mode.

Step 11 Access the global configuration mode by entering the configuration terminal.

Step 12 Import the CVP CallServer Certificate to Cisco IOS Gateway by entering the following commands:

```
crypto pki trustpoint <Call Server trust point name>
enrollment terminal

exit
```

Step 13 Open the exported Call Server certificate in Notepad and copy the certificate information that appears between the -BEGIN CERTIFICATE and END CERTIFICATE tags to the IOS device.

Step 14 Enter the following command:

```
crypto pki auth <Call Server  trust point name>
```

Step 15 Paste the certificate from Notepad and end with a blank line or the word *quit* on a line by itself.

Step 16 To generate the self-signed certificate of the Gateway, first generate 2048-bit RSA keys:

```
crypto key generatersageneral-keys Label <Your Ingress GW trustpointname> modulus 2048
```

Step 17 Configure a trustpoint:

```
crypto pkitrustpoint<Your Ingress GW trustpointname>
enrollment selfsigned
fqdn none
subject-name CN=SIP-GW
rsakeypair <Your Ingress GW trustpoint name>

Router(config)# crypto pkienroll<Your Ingress GW trustpointname>
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

Step 18 View the certificate in PEM format, and copy the Self-signed CA certificate (output starting from "----BEGIN" to "CERTIFICATE----") to a file named *ingress_gw.pem*.

```
Router(config)# crypto pki export <Your Ingress GW trustpoint name> pem terminal
% Self-signed CA certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAVSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
R1cwHhcNMTcwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxkMj7X3I6ijaL2Oll2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsE1AbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
```

```
VR0jBBgwFoAU+tJphvbvgc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBBQUAA4GBADRaW93OqErMEgRGWJJVLlbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOEc6eHUKCHoks1FDV211MMlzPe7MAc
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/l74nlT
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB6zCCAVSgAwIBAgIBAjANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZTSVAt
R1cwHhcNMTcwOTI2MTQ1MTE2WhcNMjAwMTAxMDAwMDAwWjARMQ8wDQYDVQQDEwZT
SVAtR1cwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAKdSDxIj8T6UaYxgujMk
9B2d5dq3Ni8s1e4yfsSB1lbJ/AQk+aLDfE3/BeVkeXEjRCohhnZcEnMV4DdOPxj7
9MWzoJgxkMj7X3I6ijaL2Oll2iQuBcjiqYtAUPlxB3VTjqLMbxG30fb7xLCDTuo5
s07TLsE1AbxrbrH62Za/C0e5AgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMBAf8wHwYD
VR0jBBgwFoAU+tJphvbvgc7yE6uqIh7VlgTrtPswHQYDVR0OBBYEFPrSaYb274HO
8hOrqiIe1ZYE67T7MA0GCSqGSIb3DQEBBQUAA4GBADRaW93OqErMEgRGWJJVLlbs
n8XnSbiw1k8KeY/AzgxBoBJtc0FKs4L0XUOEc6eHUKCHoks1FDV211MMlzPe7MAc
vDd7EV/abx2UdFSL9jjm/YzIleVUj8b0T3qNSfOqDtV5CyCjPichNa2eCR1bTmGx
o3HqLeEl/+66L/l74nlT
-----END CERTIFICATE-----
```

Step 19 Test your certificate.

```
show crypto pkicertificates
```

Step 20 To configure TLS version on the Gateway:

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>
v1.0 Enable TLS Version 1.0
v1.1 Enable TLS Version 1.1
v1.2 Enable TLS Version 1.2

Note: SIP TLS version 1.2 is available in Cisco IOS Software Release 15.6(1)T and higher.
```

Step 21 To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

Step 22 To enable SRTP on the incoming/outgoing dial-peer, specify SRTP:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp

Note: This command is supported in Cisco IOS Software Release 15.6(1)T and higher.
```

Step 23 Configure the SIP stack in Cisco IOS GW to use the self-signed certificate of the router to establish a SIP TLS connection from/to the CVP Call Server.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address> <peer subnet mask>
trustpoint <Your Ingress GW trustpoint name> strict-cipher

Example:
sip-ua
 crypto signaling remote-addr 10.48.54.89 255.255.255.255 trustpoint VG-SIP-1 strict-cipher
```

Step 24 Configure an outbound VoIP dial-peer to route calls to the CVP Call Server.

```
session target ipv4:<Call Server IP address>:5061
 session transport tcp tls

Example:
dial-peer voice 3 voip
 destination-pattern 82...
 session protocol sipv2
 session target ipv4:10.48.54.89:5061
 session transport tcp tls
 dtmf-relay rtp-nte
 codec g711ulaw
```

Step 25 To import GW or CUSP certificate into the CVP Call Server:

a) Copy the Ingress GW/CUSP self-signed certificate to `%CVP_HOME%\conf\security\` and import the certificate to the callserverkeystore. **%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetypeJCEKS -alias gw_cert -file %CVP_HOME%\conf\security\<ingress GW\CUSP certificate name>**

b) Enter the keystore password when prompted.

c) A message appears on the screen: `Trust this certificate? [no]:` Enter **yes**.

d) Use the list flag to check your keystore entries by running **%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -list**

Step 26 To change the supported TLS version from Unified CCE Administration, see CVP Server Services Setup, on page 24.

Step 27 Restart the Call Server.

CA-Signed Certificate

For the configuration steps, see the latest *Cisco Unified Border Element Configuration Guide* available at https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/products-installation-and-configuration-guides-list.html.

Before you begin

- To configure SIP TLS and SRTP on the gateway, apply a security-k9 license on the gateway.
- Time sync all the nodes (CVP, VVB, Gateway) with an NTP server.

Procedure

Step 1 Create a 2048-bit RSA key.

```
Router(config)# crypto key generate rsa general-keys Label <name of the key pair> modulus
2048
   Generates 2048 bit RSA key pair.
```

Step 2 Create a trustpoint. A trustpoint represents a trusted CA.

Example:

```
Router(config)# crypto pki trustpoint ms-ca-name
     Creates the trustpoint.
```

```
Router(config-pki-trustpoint)# enrollment terminal
    Specifies cut and paste enrollment with this trustpoint.

Router(config-pki-trustpoint)# subject-name CN=sslvpn.mydomain.com,OU=SSLVPN,O=My Company
Name,C=US,ST=Florida
    Defines x.500 distinguished name.

Router(config-pki-trustpoint)# rsakeypair keypairname
    Specifies key pair generated previously

Router(config-pki-trustpoint)# fqdn sslvpn.mydomain.com
   Specifies subject alternative name (DNS:).

Router(config-pki-trustpoint)# exit
```

Step 3 Create a CSR (Certificate Request) to give to the MS Certificate Server.

Example:

```
Router(config)# crypto pki enroll ms-ca-name
% Start certificate enrollment ..
% The subject name in the certificate will include: CN=Webvpn.cisco.com
% The subject name in the certificate will include: webvpn.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Display Certificate Request to terminal? [yes/no]: yes
! Displays the PKCS#10 enrollment request to the terminal.
! You will need to copy this from the terminal to a text
! file or web text field to submit to the 3rd party CA.

Certificate Request follows:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Redisplay enrollment request? [yes/no]: no

Router(config)#
```

Step 4 Sign the CSR with the root CA.

Step 5 Install the root certificate.

```
Router(config)# crypto pki authenticate ms-ca-name
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-----END CERTIFICATE-----
quit

Certificate has the following attributes:
Fingerprint MD5: D5DF85B7 9A5287D1 8CD50F90 232DB534
Fingerprint SHA1: 7C4656C3 061F7F4C 0D67B319 A855F60E BC11FC44
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

Step 6 Install the signed certificate for the gateway:

```
Router(config)# crypto pki import ms-ca-name certificate
```

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

-----END CERTIFICATE-----
quit
% Router Certificate successfully imported
```

Step 7 Test your certificate.

```
show crypto pki certificates
```

Note

- To configure TLS version on the gateway:

```
router#
router# config terminal
router(config)# sip-ua
router(config-sip-ua)# transport tcp tls <version>
  v1.0  Enable TLS Version 1.0
  v1.1  Enable TLS Version 1.1
  v1.2  Enable TLS Version 1.2
```

- To check if the TLS version is negotiated:

```
router# show sip-ua connections tcp tls detail
```

- To enable SRTP on the incoming/outgoing dial-peer, specify srtp:

```
router# configure terminal
router(config)# dial-peer voice 100 voip
router(config-dial-peer)# srtp
```

Step 8 Associate the created trustpoint in Step 2 with sip-ua.

```
router# configure terminal
router(config)# sip-ua
router(config-sip-ua)# crypto signaling remote-addr <peer IP address>
<peer subnet mask> trustpoint <trust point name created in step2>
```

Note Installing CVP Call/VXML Servers enables IIS (for media server functionality), which opens port 443 by default for TLS connections. This port allows TLSv1.0 and TLSv1.1 connections. To close these connections, change the **Enabled** value to 0 by selecting the **Decimal** option in the following registry keys:

- **TLSv1.0:** `HKEY-LOCAL-MACHINE \SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL\Protocols\TLS1.0\Server\Enabled`
- **TLSv1.1:** `HKEY-LOCAL-MACHINE\ SYSTEM\CurrentControlSet\Control\SecurityProviders\ SCHANNEL\Protocols\TLS1.1\Server\Enabled`

This disables ports 443 and 3389 for TLSv1.0 and TLSv1.1 server-side connections. While Windows 8 and Windows Server 2012 remote desktop clients work by default, Windows 7 and Windows Server 2008 remote desktop clients cannot connect to these servers for the RDP port (3389). To re-enable this port, install the patch available at https://support.microsoft.com/en-us/help/3080079/update-to-add-rds-support-for-tls-1-1-and-tls-1-2-in-windows-7-or-wind.

Secure Communication on CUSP

You can secure communication on CUSP by:

- Exchanging the self-signed certificates between the components.
- Signing the certificates by a Certificate Authority.

Self-Signed Certificate

For the configuration steps, see the latest *CLI Configuration Guide for Cisco Unified SIP Proxy* https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusp/rel9_0/cli_configuration/cusp_cli_config/configuration.html#72360.

CA-Signed Certificate

Procedure

Step 1 Create an RSA keypair in CUSP. From the CUSP foundation, enter the config mode and create the keypair:

democusp48(config)# crypto key generate rsa label <key-label> modulus 2048 default

Example

```
democusp48# conf terminal
democusp48(config)# crypto key generate rsa label cusp48-ca modulus 2048 default
Key generation in progress. Please wait...
The label name for the key is cusp48-ca
```

Step 2 Generate CSR signed by CA by running **democusp48(config)# crypto key certreq label <key-label> url ftp:**

An FTP or HTTP server is required to export the CSR. Make sure the label in the command matches the label used to create the rsa private key.

Example

```
democusp48(config)# crypto key certreq label cusp48-ca url ftp:
Address or name of remote host? 10.64.82.176
Username (ENTER if none)? test
Password (not shown)?
Destination path? /cusp48-ca.csr Uploading CSR file succeed
democusp48(config)#
```

Step 3 Import the CA server root certificate into CUSP by running: **crypto key import trustcacert label <rootCA-label> terminal**.

Example

```
democusp48(config)# crypto key import trustcacert label rootCA terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIEdTCCA12gAwIBAgIQaO1+pgDsy5lNqtF3E
epB4TANBgkqhkiG9w0BAQUFADBC MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYK
CZImiZPyLGQBGRYHQVJUR1NPTDES MBAGA1UEAxMJU0lQUEhPTklYMB4XDTA3MDc
xMzExNTAyMVoXDTEyMDcxMzExNTgz MVowQjETMBEGCgmSJomT8ixkARkWA2NvbT
EXMBUGCgmSJomT8ixkARkWB0FSVEdT T0wxEjAQBgNVBAMTCVNJUFBIT05JWDCCA
SIwDQYJKoZIhvcNAQEBBQADggEPADCC AQoCggEBAKbepxqDVZ5uWUVMWx8VaHVG
geg4CgDbzCz8Na0XqI/0aR9lImgx1Jnf ZD0nP1QvgUFSZ2m6Ee/pr2SkJ5kJSZo
zSmz2Ge4sKjZZbgQHmljWv1DswVDw0nyV F71ULTaNpsh81JVF5t2lqm75UnkW4x
P5qQn/rgfXv/Xse9964kiZhZYjtt2Ixt2V3imhh1i228YTihnTY5c3L0vD30v8dH
newsaCKd/XU+czw8feWguXXCTovvXHIbFeHvLCk9FLDoV8n9PAIHWZRPnt+HQjsD
s+jaB3F9MPVYXYElpmWrpEPHUPNZG4LsFi 6tQtiRP2UANUkXZ9fvGZMXHCZOZJi
FUCAwEAAaOCAWUwggFhMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA
1UdDgQWBBR39nCk+FjRuAbWEof5na/+Sf58STCCAQ4GA1UdHwSCAQUwggEBMIH+o
IH7oIH4hoG4bGRhcDovLy9DTj1TSVBQSE9O SVgsQ049U0lQUEhPTklYLUlORElB
LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBT ZXJ2aWNlcyxDTj1TZXJ2aWNlcyx
DTj1Db25maWd1cmF0aW9uLERDPUFSVEdTT0ws REM9Y29tP2NlcnRpZmljYXRlUm
V2b2NhdGlvbkxpc3Q/YmFzZT9vYmplY3RDbGFz cz1jUkxEaXN0cmlidXRpb25Qb
2ludIY7aHR0cDovL3NpcHBob25peC1pbmRpYS5h cnRnc29sLmNvbS9DZXJ0RW5y
b2xsL1NJUFBIT05JWC5jcmwwEAYJKwYBBAGCNxUB BAMCAQAwDQYJKoZIhvcNAQE
FBQADggEBAHua4/pwvSZ48MNnZKdsW9hvuTV4jwtGErgc16bOR0Z1urRFIFr2NCP
yzZboTb+ZllkQPDMRPBoBwOVr7BciVyoTo7AKFheqYm9asXL18A6XpK/WqLjlCcX
rdzF8ot0o+dK05sd9ZG7hRckRhFPwwj5Z7z0Vsd/jcO51QjpS4rzMZZXK2FnRvng
d5xmp4U+yJtPyr8g4DyAP2/UeSKe0SEYoTV5x5FpdyF4veZneB7+ZfFntWFf4xwi
obf+UvW47W6pCj5nGLMBzOiaxeQ8pre+yjipL2ucWK4ynOfKzz4XlkfktITDSogQ
A1AS1quQVbKTKk+qLGD6Ml2P0LrcKQkk=
-----END CERTIFICATE-----
Certificate info
****************************************
Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03
Do you want to continue to import this certificate, additional validation will be perfom?
[y/n]: y
democusp48(config)#
```

Step 4 Import the signed certificate into CUSP by running **crypto key import cer label <key-label> url terminal**.

Example

```
democusp48(config)# crypto key import cer label cusp48-ca terminal
Enter certificate...
End with a blank line or "quit" on a line by itself
-----BEGIN CERTIFICATE----- MIIFITCCBAmgAwIBAgIKGI1fqgAAAAAAEDAN
BgkqhkiG9w0BAQUFADBCMRMwEQYK CZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZ
PyLGQBGRYHQVJUR1NPTDESMBAGA1UE AxMJU0lQUEhPTklYMB4XDTA4MTIwOTA5M
```

```
DExOVoXDTA5MTIwOTA5MTExOVowYTEL MAkGA1UEBhMCJycxCzAJBgNVBAgTAicn
MQswCQYDVQQHEwInJzELMAkGA1UEChMC JycxCzAJBgNVBAsTAicnMR4wHAYDVQQ
DExVTT0xURVNUQ0MuYXJ0Z3NvbC5jb20w gZ8wDQYJKoZIhvcNAQEBBQADgY0AMI
GJAoGBAOZz88nK51bJYjWgvuv4Wx1CGxTN YWGyNg+vDyQgKBXlL7b1CqBxlYjl4
eetO4LiKkW/y4jSv3nCxCAdOrMvVF5lxFmY baMlR1R/qMCLzAMvmsWlH6VY4rcf
FGkjed3zCcI6BJ6fG9H9dt1J+47iM7SdZYz/ NrEqDnrpoHaUxdzlAgMBAAGjggJ
8MIICeDAdBgNVHQ4EFgQUYXLxMfiZJP29UZ3w Mpj0e79sk4EwHwYDVR0jBBgwFo
AUd/ZwpPhY0bgG1hKH+Z2v/kn+fEkwggEOBgNV HR8EggEFMIIBATCB/qCB+6CB+
IaBuGxkYXA6Ly8vQ049U0lQUEhPTklYLENOPVNJ UFBIT05JWC1JTkRJQSxDTj1D
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMs Q049U2VydmljZXMsQ049Q29
uZmlndXJhdGlvbixEQz1BUlRHU09MLERDPWNvbT9j ZXJ0aWZpY2F0ZVJldm9jYX
Rpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9YlJMRGlz dHJpYnV0aW9uUG9pbnSGO
2h0dHA6Ly9zaXBwaG9uaXgtaW5kaWEuYXJ0Z3NvbC5j b20vQ2VydEVucm9sbC9T
SVBQSE9OSVguY3JsMIIBIgYIKwYBBQUHAQEEggEUMIIB EDCBqAYIKwYBBQUHMAK
GgZtsZGFwOi8vL0NOPVNJUFBIT05JWCxDTj1BSUEsQ049 UHVibGljJTIwS2V5JT
IwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJh dGlvbixEQz1BUlRHU
09MLERDPWNvbT9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0 Q2xhc3M9Y2VydGlm
aWNhdGlvbkF1dGhvcml0eTBjBggrBgEFBQcwAoZXaHR0cDov L3NpcHBob25peC1
pbmRpYS5hcnRnc29sLmNvbS9DZXJ0RW5yb2xsL1NJUFBIT05J WC1JTkRJQS5BUl
RHU09MLmNvbV9TSVBQSE9OSVguY3J0MA0GCSqGSIb3DQEBBQUA A4IBAQAXm0MPu
eXcMYxQhVlPR/Yaxw0n2epeNRwsPP31Pr9Ak3SYSzhoMRVadJ3z K2gt4qiVV8wL
tzTO2o70JXKx+0keZdOX/DQQndxBkiBKqdJ2Qvipv8Z8k3pza3lN jANnYw6FL3/
Yvh+vWCLygEHfrUfKj/7H8GaXQVapj2mDs79/zgoSyIlo+STmwFWT GQy6iFO+pv
vMcyfjjv2dsuwt1Ml0nlict0LtkIKnRGLqnkA6sJo1P6kE+WK7n3P2 yho/Lg98q
vWl+1FRC18DrkUhpNiKXsP1ld9TcJGrdJP9zG7lI5Mf3Q/2NIAx2JZd ZVAsXZMN
smOsOrgXzkcU/xU3BXkX -----END CERTIFICATE-----  Import succeeded
democusp48(config)#exit
democusp48#
```

Step 5 You can list the certificates by running **show crypto key all**.

Example

```
democusp48# sh crypto key all
Label name: rootca
Entry type: Trusted Certificate Entry
Creation date: Sat Jul 01 14:13:14 GMT+05:30 2017
Owner: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
Valid from: Wed Mar 22 14:23:10 GMT+05:30 2017 until: Tue Mar 22 14:33:09 GMT+0
5:30 2022
Certificate fingerprint (MD5): 41:A2:31:9D:97:AF:A8:CA:60:FC:46:95:82:DE:78:03

Label name: cusp48-ca
Entry type: Key Entry
Creation date: Tue Jul 04 10:47:40 GMT+05:30 2017
Owner: CN=democusp48.cvpvb.cisco.com, OU='', O='', L='', ST='', C=''
Issuer: CN=cvpvb-GDESINGHROOTCA-CA, DC=cvpvb, DC=cisco, DC=com
SubjectAltName: DNS:democusp48.cvpvb.cisco.com
Valid from: Tue Jul 04 10:41:56 GMT+05:30 2017 until: Thu Jul 04 10:41:56 GMT+0
5:30 2019
Certificate fingerprint (MD5): 91:ED:83:CA:3B:37:16:E8:AB:07:EA:85:04:1A:D1:05
```

Configure Media Server

The following instructions are applicable for the Media Server installed in CVP and also for the Media Server installed as a seperate server.

Procedure

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

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

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

Step 4 Goto **Connections** panel:

a) Expand CVP server that you want to add FTP site.

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

Step 5 Enter **FTP Site Name**.

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

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

Step 8 Enter **Port** number.

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

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

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

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

Configure Basic Settings for FTP Server

Procedure

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

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

Step 3 Click **Connect As**.

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

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

Configure CVP Reporting Server

Reporting provides historical reporting to a distributed self-service deployment in a call center. The CVP Reporting Server receives the reporting data from one or more CVP Servers and CVP VXML Servers, and stores that data in an Informix database. The call data is stored in a relational database, on which you can write custom reports. The administrators can schedule data removal (delete) and database backups. Multiple CVP Call Servers can send data to a single CVP Reporting Server.

Reporting Server Users and Passwords

You can manage Reporting Server Users and Passwords using Windows Operating System Local User Management.

Note Please turn off all the Cisco services and IDs services on the CVP reporting server.

You can do this by using **Local Users and Groups** within the **Computer Management** console. To access this console, navigate to **Start** > **Administrative Tools** > **Computer Management**.

Changing Database User Passwords

You can change the password of Reporting Server database users. Navigate to **Computer Management** > **Local Users and Groups** > **Users**, choose **cvp_dbadmin (Database Administrator)** or **cvp_dbuser (Database User)**, then right click and select **Set Password**.

Associating Database User Passwords

You can associate the password of Reporting Server database users.

1. In the reporting server from the command prompt, navigate to the **C:\Cisco\CVP\bin** directory.
2. Run the command **report-init.bat -reporthashpwYourPassword** (same password that you set).
3. The **report-init.bat** command encrypts the **cvp_dbadmin** and **cvp_dbuser** passwords and stores them in the *reporting.properties* file that is located at the **C:\Cisco\CVP\conf** folder on the CVP Reporting server. The **RPT.DBPassword** and **RPT.DBAdminPassword** get updated in this process.

Note The password must meet all the reporting password requirements. You can ignore log4J errors which appear after executing this command.

4. Verify if the *reporting.properties* file is updated. The passwords for **cvp_dbadmin** and **cvp_dbuser** are encrypted.
5. Restart the CVP Reporting server and access the CVP Informix DB through **cvp_dbadmin** and **cvp_dbuser** accounts to verify the update.
6. Make a test call to verify if the data is getting populated.

Managing Reporting Server Users

You can add, modify, or delete the Reporting Server users. Navigate to **Computer Management** > **Local Users and Groups** > **Users**.

If you need database access, you can add your name to the **Informix-Admin** group.

Configure Reporting Properties

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Reporting Server**.

Step 2 Click the **Properties** tab. Complete the following fields:

Table 10: Reporting Server Properties

Field	Required?	Description
Trunk Utilization		
Enable Reporting	-	Enables the Reporting Server to receive call data from the associated CVP Servers.
Maximum File Size	no	Defines the maximum size of the file used to record the data feed messages during a database failover. This can be limited by the amount of free disk space. Default is 100MB. Range is 1 to 250.

Step 3 Click **Save**.

Configure Database

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Reporting Server**.

Step 2 Click the **Database Configuration** tab. Complete the following fields:

Table 11: Database Configuration Properties

Field	Required?	Description
Schedule Daily Backups	-	Schedules backups of the Reporting database or runs backups on demand. When you enable backups, the files are saved to the Reporting Server's local file system. You are responsible for managing the backed-up files. The scheduled backups occur once each day. You can configure the time of day for the backups. A maximum of two backups and a minimum of one backup are available at any time on the local machine.
DB Admin Password	yes	The password for the Reporting Database administrator.
Data Retention		
Trunk Utilization Usage	yes	Retention days for the Gateway Trunk Utilization reporting data. Default is 15 days.
Call	yes	Detailed information about the calls received by Unified CVP. Default is 30 days.

Field	Required?	Description
Call Event	yes	Call state change event messages published by the Call Server and the CVP VXML Server. SIP and IVR Services publish call state change event messages when a SIP call changes its state. These states include call initiated, transferred, terminated, stopped, or error state. Default is 30 days.
Callback	yes	Retention days for the Courtesy Callback reporting data. Default is 15 days.
VoiceXML Session	yes	The VXML session data includes application names, session ID, and session variables. The session variables are global to the call session on the CVP VXML Server. Unlike element data, session data can be created and modified by all components (except the global error handler, hot events, and XML decisions). Default is 15 days.
VoiceXML Element	yes	A VXML element is a distinct component of a voice application call flow whose actions affect the caller experience. A VXML element contains the detailed script activity to the element level, such as Call Identifiers, activity timestamp, VXML script name, name and type of the VXML element, and event type. Default is 15 days.
VoiceXML ECC Variable	yes	Expanded Call Context (ECC) variables that are included in the VXML data. Unified CVP uses the ECC variables to exchange information with Unified ICME. Default is 15 days.
VoiceXML Voice Interact Detail	yes	The application detailed data at the script element level from the CVP VXML Server call services. This data includes input mode, utterance, interpretation, and confidence. Default is 15 days.
VoiceXML Session Variable	yes	The VXML session variables are global to the call session on the CVP VXML Server. Default is 15 days.
VoiceXML Element Detail	yes	The names and values of the element variables. Default is 15 days.
Set Time for Purging Data	no	The time set for purging data.

Step 3 Click **Save**.

Set Up Reporting Server Infrastructure

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Reporting Server**.

Step 2 Click the **Infrastructure** tab. Complete the following fields:

Table 12: Infrastructure Properties

Field	Required?	Description
Configuration: Thread Management		
Maximum Threads	yes	The maximum thread pool size in the Reporting Server Java virtual machine. Default is 525. Range is 100 to 1000.
Advanced		
Statistics Aggregation Interval	yes	The interval at which the CVP Reporting Server publishes statistics. Default is 30 minutes. Range is 10 to 1440.
Log File Properties		
Maximum Log File Size	yes	The maximum size of the log file in megabytes. The log file name follows this format: **CVP.DateStamp.SeqNum.log** For example: **CVP.2006-07-04.00.log** After midnight each day, a new log file is automatically created with a new date stamp. When a log file exceeds the max log file size, a new one with the next sequence number is created, for example, when **CVP.2006-07-04.00.log** reaches 5MB, **CVP.2006-07-04.01.log** is automatically created. Default is 10MB. Range is 1 to 100.
Maximum Log Directory Size	yes	The maximum size of the directory containing the CVP Reporting Server log files. **Note** Modifying the value to a setting that is below the default value might cause the logs to be quickly rolled over. Consequently, the log entries might be lost, which can affect troubleshooting. Default is 20000MB. Range is 500 to 500000.
Configuration: Primary Syslog Server Settings		

Field	Required?	Description
Primary Syslog Server	no	The hostname or the IP address of the primary syslog server to send the syslog events from a CVP application.
Primary Syslog Server Port Number	no	The port number of the primary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Primary Backup Syslog Server	no	The hostname or the IP address of the primary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.
Primary Backup Syslog Server Port Number	no	The port number of the primary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Configuration: Secondary Syslog Server Settings		
Secondary Syslog Server	no	The hostname or the IP address of the secondary syslog server to send the syslog events from a CVP application.
Secondary Syslog Server Port Number	no	The port number of the secondary syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.
Secondary Backup Syslog Server	no	The hostname or the IP address of the secondary backup syslog server to send the syslog events from a CVP application when the syslog server cannot be reached.
Secondary Backup Syslog Server Port Number	no	The port number of the secondary backup syslog server. It can be any available port number. Valid port numbers are integers between 1 and 65535.

Step 3 Click **Save**.

Associate Unified CVP Call Servers with CVP Reporting Server

To store the call data that are handled by Call Servers in the Reporting Database, you must associate CVP Call Servers with CVP Reporting Server.

Note A Unified CVP Reporting Server can have one or more CVP Call Servers. However, a Unified CVP Call Server can only be associated with one CVP Reporting Server.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **CVP Reporting Server**.

Step 2 Click the **Call Server Association** link.
The **Call Server Association** popup window opens.

Step 3 Select a **Reporting Server** from the drop-down list. The list includes all the Reporting Servers available in the Packaged CCE inventory.

Step 4 To associate CVP Call Servers with the selected CVP Reporting Server:

a) Click the + icon to open the **Add CVP Call Server(s)** popup. The popup includes a list of CVP Call Servers that are available for reporting association.

b) Select one or more Call Servers from the list and close the popup.
The selected Call Servers appear in the **Configured Call Servers** table.

Step 5 Click **Save**.

You can continue to associate other CVP Reporting Servers with available Call Servers.

Step 6 Click **Cancel** to return to the **Device Configuration** page.

Cisco Virtualized Voice Browser (VVB) Setup

Cisco Virtualized Voice Browser (Cisco VVB) provides a platform for interpreting VXML documents. When an incoming call arrives at the contact center, Cisco VVB allocates a VXML port that represents the VoIP endpoint. Cisco VVB sends HTTP requests to the Unified CVP VXML server. The Unified CVP VXML server runs the request and sends back a dynamically generated VXML document.

Note After fresh install, add VVB to the System Inventory as an external device.

After Packaged CCE Fresh Install, you can configure the following Virtualized Voice Browser settings for the site:

- Configure Media Parameters
- Configure Security Parameters
- Configure Automatic Speech Recognition (ASR) and Text-to-Speech (TTS) servers.
- Configure the default applications types - Comprehensive, Ringtone, and Error, and add SIP triggers to invoke the application.

Configure Media and Security Parameters

To configure media and security parameters, add audio codec and MRCP version, and enable TLS and Secure Real-Time Transport Protocol (SRTP).

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **Virtualized Voice Browser**.

Step 2 Select the site name from the list for which you want to set up the VVB media and security parameters. By default, it is 'Main'.

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

Field	Required ?	Description
Media Parameters **Note** If you change a configuration, you must restart the VVB engine.		
Codec	Yes	G711 (U-law, A-law) and G729 Audio Codecs are supported. Default codec is G711U.
MRCP Version	Yes	Select the version of the MRCP protocol to communicate between Nuance (ASR/TTS) and Cisco VVB. Default is MRCPv2. **Note** ASR-TTS service is not supported using G729 codec; therefore, MRCP is not applicable for this codec.
User prompts override system prompts	-	By default, this feature is disabled. Click to allow the custom recorded prompts override the system default prompts. When enabled, the system plays the custom recorded prompt that is uploaded to the appropriate language directory.
Security Parameters **Note** If you change a configuration, you must restart the VVB engine.		
TLS(SIP)	Yes	TLS is disabled by default. Click to enable the secure SIP signalling on the IVR leg.
TLS (SIP) Version	Yes	**Note** Enable **TLS(SIP)** to use this security parameter. Choose the minimum TLS version of SIP to be supported from the drop-down list. Default value is TLSv1.2.
Cipher Configuration	Yes	**Note** Enable **TLS(SIP)** to use this security parameter. The default cipher TLS_RSA_WITH_AES_128_CBC_SHA is available in the **Cipher Configuration** list. The default cipher is mandatory for TLS version 1.2 and cannot be deleted. **a.** Click the + icon and enter the ciphers to be supported by Cisco VVB, with key size lesser than or equal to 1024 bits. Cipher support is as per Java Virtual Machine (JVM). **b.** Click **Add**

Field	Required ?	Description
SRTP	-	**Note** Enable **TLS(SIP)** to use this security parameter. By default, SRTP is disabled. Enable SRTP to secure media on the IVR leg. When SRTP is enabled, the IVR media is encrypted. SRTP uses Crypto-Suite AES_CM_128_HMAC_SHA1_32 for encrypting the media stream.
Allow RTP(Mixed Mode)	-	**Note** Enable **TLS(SIP)** and **SRTP**to use this security parameter. **Allow RTP (Mixed Mode)** is available when you enable **SRTP**. Enable **Allow RTP (Mixed Mode)** if a nuance device is configured to work in the RTP mode. When enabled, VVB accepts both SRTP and RTP call flows.

Step 4 Click **Save**.

Configure Speech Servers

Cisco VVB uses the Automatic Speech Recognition (ASR) and Text-To-Speech (TTS) speech servers. The ASR and TTS configurations involve specifying the hostname or IP address of the respective speech servers.

Before you begin

Order ASR and TTS speech servers from Cisco-supported vendors. To provision, install, and configure the ASR and TTS speech server software, consult the vendor's application requirement.

Note For more information about supported speech servers for Cisco VVB, see the Solutions Compatibility Matrix available at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-device-support-tables-list.html

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **Virtualized Voice Browser**.

Step 2 Select the site name from the list for which you want to set up the VVB media and security parameters. By default, it is 'Main'.

Step 3 Click the **Speech Servers** tab.

Step 4 Complete the following fields on the **Speech Servers** tab:

Fields	Required?	Description
ASR Servers		

Fields	Required?	Description
Configured ASR Servers	No	**a.** Click the '+' icon and enter the hostname or IP address of ASR server. **b.** Click **Add**.
TTS Servers		
Configured TTS Servers	No	**a.** Click the '+' icon and enter the hostname or IP address of TTS server. **b.** Click **Add**.

Configure Default Application Properties

Cisco VVB includes the call flow deployment models (applications) to support different business needs. Any VVB in PCCE deployment can be configured with the following three predefined applications:

- Comprehensive application
- Ringtone application
- Error application

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Infrastructure Settings** > **Device Configuration** > **Virtualized Voice Browser**.

Step 2 Select the site name from the list for which you want to set up the VVB media and security parameters. By default, it is 'Main'.

Step 3 Click the **Applications & Triggers** tab.

Step 4 Complete the following on the **Applications & Triggers** tab:

- To configure **Comprehensive** application

Field	Required?	Description
Application	Yes	From the **Application** drop-down list, choose **Compre**

Field	Required?	Description
Sigdigits	No	Enter the number of digits that are used as the signif Range is 0 to 20. The call arrives at Unified CVP with the significa (SigDigit) prepended to the Dialed Number (DN) CVP strips the digits and transfers the call to the U When ICM returns the label to Unified CVP to ro to Cisco VVB, Unified CVP prepends the digits a Cisco VVB uses the SigDigit configuration on the Comprehensive application to remove the prepend that when the IVR leg of the call is set up, the ori is used on the incoming VoiceXML request.
Maximum Sessions	Yes	Enter the number of sessions you like to associate application. Range is 1 to 600. **Note** The number of sessions must be less the license provided by Cisco VVB.
Enable HTTPS	No	By default, the Enable HTTPS option is disabled. Click to enable the option. When enabled, the com between the Cisco VVB and VXML server is enc If you have enabled secure communication, then • Upload the relevant certificate. To upload the see the Upload certificate or certificate trust *Cisco Unified Communications Operating Sy Administration Guide*. • Restart VVB services using the VVB Admin **Unified Serviceability** > **Tools** > **Control C Network Services**) or the system CLI comm **service restart Cisco Tomcat**".

Field	Required?	Description
Configured Triggers	Yes	The field contains default SIP trigger configured for t **Comprehensive** application. See Default SIP Trigger To add a new trigger: **a.** Click the '+' icon, and enter a new SIP trigger to l associated with the application. Valid input characters are alphanumeric (0-9, x, X period (.), exclamation (!), asterisk (*), and greate (>). An error message appears for an invalid inpu **b.** Click **Add**. The trigger appears in the **Configure** **Triggers** list. **Note** On adding a SIP trigger, push the trigger t from the **Device Configuration** page for appear in the **Configured Triggers** list. To remove a trigger from the list, click the 'x' icon tha associated with the trigger in the list.

- To configure **Ringtone** application

Field	Required?	Description
Application	Yes	From the **Application** drop-down list, choose Ringtone.
Maximum Sessions	Yes	Enter the number of sessions you like to associate with the application. Range is 1 to 600. **Note** The number of sessions must be less or equal to the license provided by Cisco VVB.
Configured Triggers	Yes	The field contains default SIP trigger configured for the **Ringtone** application. See Default SIP Triggers. To add a new trigger: **a.** Click the '+' icon, and enter a new SIP trigger to be associated with the application. Valid input characters are alphanumeric (0-9, x, X, T), and the special characters like period (.), exclamation (!), asterisk (*), and greater than (>). An error message appears for an invalid input. **b.** Click **Add**. The trigger appears in the **Configured Triggers** list. **Note** On adding a SIP trigger, push the trigger to VVB from the **Device Configuration** page for it to appear in the **Configured Triggers** list. To remove a trigger from the list, click the 'x' icon that is associated with the trigger in the list.

- To configure **Error** application

Field	Required?	Description
Application	Yes	From the **Application** drop-down list, choose Error.
Maximum Sessions	Yes	Enter the number of sessions you like to associate with the application. Range is 1 to 600. **Note** The number of sessions must be less or equal to the license provided by Cisco VVB.
Custom error prompt	No	Provide the custom error .wav file to play. **Note** The field is case-sensitive. The prompt file must be uploaded to Cisco VVB. If custom prompts are not uploaded or found, the default prompt is played.
Configured Triggers	Yes	The field contains default SIP trigger configured for the **Error** application. See Default SIP Triggers. To add a new trigger: **a.** Click the '+' icon, and enter a new SIP trigger to be associated with the application. Valid input characters are alphanumeric (0-9, x, X, T), period (.), exclamation (!), asterisk (*), and greater than (>). An error message appears for an invalid input. **b.** Click **Add**. The trigger appears in the **Configured Triggers** list. **Note** On adding a SIP trigger, push the trigger to VVB from the **Device Configuration** page for it to appear in the **Configured Triggers** list. To remove a trigger from the list, click the 'x' icon associated with the trigger in the list.

Step 5 Click **Save**.

Default SIP Triggers

The pre-defined applications have the default SIP triggers as shown in the table.

Table 13: Default SIP Triggers

Application	Description	Pre-configured SIP Trigger
Comprehensive	Used for comprehensive calls	7777777777*
Ringtone	Used for playing ringtone and whisper	91919191*

Application	Description	Pre-configured SIP Trigger
Error	Used for playing error tone	92929292*

Finesse

Use this page to configure the following settings for Cisco Finesse administration:

- IP Phone Agent
- CTI Server
- Administration and Data Server
- Cluster Settings

Note The CTI Server, Administration and Data Server, and Cluster Settings are available only for Packaged CCE 4000 Agents deployment to 12000 Agents deployment.

IP Phone Agent Settings

You can set up the user credentials for an IP phone agent. Any changes that are made to these settings require a restart of Cisco Finesse Tomcat to take effect.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Infrastructure Settings** > **Device Configuration** > **Finesse** > **IP Phone Agent Settings**.

Step 2 Choose a site for the Finesse server. By default, it is Main for Packaged CCE 2000 Agents deployment.

Step 3 From the **Peripheral Set** drop-down list, select a peripheral set that has the Cisco Finesse configured for the selected **Site**.

Note The **Peripheral Set** field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set.

Step 4 Under **Phone URL Authentication Settings**, enter your **Username** and **Password**.

Step 5 Click **Save** to save your settings.

Step 6 Click **Revert** to retrieve the previously saved settings.

Related Topics

Contact Center Enterprise CTI Server Settings, on page 66
Contact Center Enterprise Administration and Data Server Settings, on page 69
Cluster Settings, on page 72

Contact Center Enterprise CTI Server Settings

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

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

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

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

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

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

The secure encryption and Test Connection functionality is supported only from Unified CCE 12.0.

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

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

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

Field	Explanation
Peripheral ID	The ID of the Agent PG Routing Client (PIM). The Agent PG Peripheral ID should be configured to the same value for the A and B Side CTI server. This field is required and accepts values between 1 and 32767. The default value is 5000.
B Side Host/IP Address	The hostname or IP address of the B Side CTI server.
B Side Port	The value of this field must match the port configured during the setup of the B Side CTI server. This field accepts values between 1 and 65535.
Enable SSL encryption	Check this box to enable secure encryption.

Actions on the Contact Center Enterprise CTI Server Settings gadget:

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

CTI Test Connection

When you click **Test Connection**:

1. Input validation is done on the request attributes.

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

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

   For information on how to establish trust between Finesse and CTI server, see *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html

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

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

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

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

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

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

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

Configure Contact Center Enterprise CTI Server Settings

Procedure

Step 1 In the Contact Center Enterprise CTI Server Settings area, enter the CTI server settings as described in the following table. Refer to your configuration worksheet if necessary.

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

Step 2 Click **Save**.

Contact Center Enterprise Administration and Data Server Settings

Use the Unified CCE Administration & Data Server Settings gadget to configure the database settings. These settings are required to enable authentication for Finesse agents and supervisors.

Note To connect to the AW Database (AWDB) in the Unified CCE Administration, Cisco Finesse supports both SQL and Windows authentication.

The Cisco Finesse Java Database Connectivity (JDBC) driver is configured to use NTLMv2. Therefore, Finesse can connect to the administration database even if the administration database is configured to use only NTLMv2.

Primary Administration & Data Server is configured on Side A and Secondary Administration & Data Server is configured on Side B. Make sure Cisco Finesse server on both sides connect to Primary Administration & Data Server on side A and fall back to Secondary Administration & Data Server on side B only when Primary Administration & Data Server goes down.

After you change and save any value on the Contact Center Enterprise Administration & Data Server Settings gadget, restart the Cisco Finesse Tomcat Service on the primary and secondary Finesse server. If you restart the Cisco Finesse Tomcat Service, agents must sign out and sign in again. To avoid this, you can make Contact Center Enterprise Administration & Data Server settings changes and restart the Cisco Finesse Tomcat service during hours when agents are not signed in to the Cisco Finesse desktop.

The following table describes the fields on the Unified CCE Administration & Data Server Settings gadget:

Table 14: Field Descriptions

Field	Description
Primary Host/IP Address	The hostname or IP address of the Unified CCE Administration & Data Server.
Backup Host/IP Address	(Optional) The hostname or IP address of the backup Unified CCE Administration & Data Server.
Database Port	The port of the Unified CCE Administration & Data Server. The default value is 1433. **Note** Cisco Finesse expects the primary and backup Administration & Data Server ports to be the same, hence the administration console exposes one port field. You must ensure that the port is the same for the primary and backup Administration & Data Servers.
AW Database Name	The name of the AW Database (AWDB). For example, *ucceinstance*_awdb).
Domain	(Optional) The domain name of the AWDB.

Field	Description
Username	The username required to sign in to the AWDB. **Note** If you specify a domain, this user refers to the Administrator Domain user that the AWDB uses to synchronize with the logger. In which case, the AWDB server must use Windows authentication and the configured username must be a domain user. If you do not specify a domain, this user must be an SQL user.
Password	The password required to sign in to the AWDB.

For more information about these settings, see the *Administration Guide for Cisco Unified Contact Center Enterprise* and the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise*.

Actions on the Unified CCE Administration & Data Server Settings gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved enterprise database settings

When you update any of the following fields and click Save, Cisco Finesse attempts to connect to the AWDB:

- Primary Host/IP Address
- Backup Host/IP Address
- Database Port
- AW Database Name

If Cisco Finesse cannot connect to the AWDB, an error message appears and you are asked if you still want to save. If you click **Yes**, the settings are saved. If you click **No**, the settings are not saved. You can change the settings and try again or click **Revert** to retrieve the previously saved settings.

When you update the Username or Password fields and click **Save**, Cisco Finesse attempts to authenticate against the AWDB. If authentication fails, an error message appears and you are asked if you still want to save. Click **Yes** to save the settings or click **No** to change the settings. Click **Revert** to retrieve the previously saved settings.

Note Finesse will not come into service in case of AWDB errors when connecting Cisco Finesse 11.5(1) and higher versions to Unified CCE 11.5(1) and higher versions.

Configure Contact Center Enterprise Administration and Data Server Settings

Configure the Unified CCE Administration & Data Server settings to enable authentication for Finesse agents and supervisors.

Procedure

Step 1 In the Unified CCE Administration & Data Server Settings area, enter the Administration & Data Server settings as described in the preceding table. For more information, see Table 14: Field Descriptions, on page 70. Refer to your configuration worksheet if necessary.

Step 2 Click **Save**.

What to do next

The CTI test functionality documented in the *Configure Unified CCE CTI Server Settings* topic depends on AWDB connectivity to determine the CTI version. Or else, the test will not go through.

Cluster Settings

Use the Cluster Settings gadget to configure a secondary Finesse server. The purpose of a secondary Finesse server is to handle all agent requests if the primary server goes down.

You must complete this configuration *before* you install the secondary Finesse server. For more information about installing a secondary Finesse server, see the *Cisco Finesse Installation and Upgrade Guide*.

The following table describes the fields on the Cluster Settings gadget:

Field	Explanation
Hostname	The hostname of the secondary Finesse server.

Actions on the Cluster Settings gadget:

- **Save:** Saves your configuration changes
- **Revert:** Retrieves the most recently saved cluster settings

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 Sign in to the administration console 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**.

Single Sign-On

Single sign-on (SSO) is an authentication and authorization process. (Authentication proves that you are the user you say that you are, and authorization verifies that you are allowed to do what you want to do.) SSO allows you to sign in to one application and then securely access other authorized applications without a

prompt to resupply user credentials. SSO permits Cisco supervisors or agents to sign on only once with a username and password. Supervisors and agents gain access to all of their Cisco browser-based applications and services within a single browser instance. By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently.

SSO is an optional feature. If you are using SSO, use the Single Sign-On tool to configure the Cisco Identity Service (IdS). You can then register and test components with the Cisco IdS, and set the SSO mode on components.

For complete instructions on setting up SSO in your deployment, see one of the following:

- *Cisco Unified Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html
- *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html
- *Installing and Configuring Guide for Cisco HCS for CC* at https://www.cisco.com/c/en/us/support/unified-communications/hosted-collaboration-solution-contact-center/products-installation-guides-list.html

Set Up the External HDS for Single Sign-On

If you have an external HDS in 2000 Agent deployments, manually associate it with a default Cisco IdS by performing the following instructions.

Procedure

Step 1 In **Unified CCE Administration**, click **Infrastructure** > **Inventory** to open the **Inventory** page.

Step 2 Click the pencil icon for the External HDS to open the edit machine popup window.

Step 3 Click the Search icon next to **Default Identity Service**.
The **Select Identity Service** popup window opens.

Step 4 Enter the machine name for the Cisco IdS in the **Search** field or choose the Cisco IdS from the list.

Step 5 Click **Save**.

Configure the Cisco Identity Service

The Cisco Identity Service (Cisco IdS) provides authorization between the Identity Provider (IdP) and applications.

When you configure the Cisco IdS, you set up a metadata exchange between the Cisco IdS and the IdP. This exchange establishes a trust relationship that then allows applications to use the Cisco IdS for single sign-on. You establish the trust relationship by downloading a metadata file from the Cisco IdS and uploading it to the IdP. You can then select settings that are related to security, identify clients of the Cisco IdS service, and set log levels. If desired, enable Syslog format.

Note In Packaged CCE 4000 or 12000 Agent deployments:

- Unified CCE AW, Unified Intelligence Center, Finesse, and external HDS gets automatically associated with a default Cisco Identity Service (Cisco IdS).
- Make sure that the Principal AW is configured, and is functional before using the Single Sign-On tool in the Unified CCE Administration. Also, add the SSO-capable machines to the Inventory.

In Packaged CCE 2000 Agent deployments, you must manually associate an external HDS with a default Cisco Identity Service (Cisco IdS). For more information, see Set Up the External HDS for Single Sign-On, on page 73.

Procedure

Step 1 In the Unified CCE Administration, choose **Overview** > **Infrastructure Settings** > **Device Configuration** > **Single Sign-On Setup**.

Note Use a log in name in the format *username@FQDN* to log in to the Unified CCE Administration.

The **Identity Service Nodes**, **Identity Service Settings**, and **Identity Service Clients** tabs appear.

Step 2 Click **Identity Service Nodes**.
You can view the overall Node level and identify which nodes are in service. You can also view the **SAML Certificate Expiry** details for each node, indicating when the certificate is due to expire. The node **Status** options are **Not Configured**, **In Service**, **Partial Service**, and **Out of Service**. Click a status to see more information. The star to the right of one of the Node names identifies the node that is the primary publisher.

Step 3 Click **Identity Service Settings**.

Step 4 Click **Security**.

Step 5 Click **Tokens**.
Enter the duration for the following settings:

- **Refresh Token Expiry** -- Refresh token is used to get new Access tokens. This parameter specifies the duration after which the Refresh token expires. The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- Authorization code is used to get Access tokens from Cisco IdS. This parameter specifies the duration after which the Authorization code expires. The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- Access token contains security credentials used to authorize clients for accessing resource server. This parameter specifies the duration after which the Access token expires. The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 6 Set the **Encrypt Token** (optional); the default setting is **On**. Use this configuration to secure the tokens as Cisco IdS issues tokens in both plain text or encrypted formats.

Step 7 Click **Save**.

Step 8 Click **Keys and Certificates**.
The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration. An Administrator regenerates the Encryption/Signature key when it is exposed or compromised.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful. SAML certificate is regenerated when it expires or when IdS relying party trust configuration on IdP is deleted.

  Note Establish the trust relationship again whenever the Encryption keys or SAML certificates are regenerated.

Step 9 Click **Save**.

Step 10 Click **Identity Service Clients**.
On the **Identity Service Clients** tab, you can view the existing Cisco IdS clients, with the client name, client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the name of client.

Step 11 To add a client on the **Identity Service Clients** tab:

a) Click **New**.
b) Enter the name of client.
c) Enter the Redirect URL. To add more than one URL, click the plus icon.
d) Click **Add** (or click **Clear** and then click the X to close the page without adding the client).

Step 12 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

- Click **Edit** to edit the client's name, ID, or redirect URL. On the **Edit Client** page, make changes and click **Save** (or click **Clear** and then click the X to close the page without saving edits).
- Click **Delete** to delete the client.

Step 13 Click **Identity Service Settings**.

Step 14 Click **Troubleshooting** to perform some optional troubleshooting.

Step 15 From the **Log Level** drop-down list, set the local log level by choosing **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 16 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the **Host** (Optional) field.

Step 17 Click **Save**.

You can now:

- Register components with the Cisco IdS.
- Enable (or disable) SSO for the entire deployment.

Application Gateway

Detailed information for Application Gateway is available in the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Peripheral Gateways

This display-only tool shows details about the peripheral gateways and peripherals in your deployment.

Click the **Site** tab to view the details of peripheral gateways and peripherals configured for that site.

Log Collection

Important Only set trace level to detailed and run log collection during off-peak hours. Do not run log collection during heavy call load.

Use the Log Collection tool to collect logs for these components:

- Unified CCE
- Unified Communications Manager
- Unified CVP
- Finesse
- Unified Intelligence Center

Unless limited by their role, administrators have full access to Log Collection. Supervisors have no access to this tool.

You can select individual or multiple components for log collection, and specify the start and end time for the logs. The maximum duration for log collection is eight hours. The logs for all selected components are consolidated into a single downloadable zip file. You can run one log collection at a time.

For most components, you can specify whether normal or detailed logs are collected using the **Trace Levels** option. Click **Trace Levels** to view the current trace level for each component and, if necessary, change it for future log collection.

The **Current Level** for each component can be Normal, Detailed, or Custom. Custom indicates that the level has been set outside of **Unified CCE Administration** and does not match the Normal or Detailed settings for that component.

System-wide trace levels are gathered periodically. If a trace level is changed outside of **Unified CCE Administration**, it may take several minutes before the new trace level appears in the **Log Collection** tool.

To use Log Collection to debug a problem:

1. In **Unified CCE Administration**, choose **Overview** > **Infrastructure Settings** > **Log Collection**.
2. To change trace level to detailed, click **Trace Levels**, and select **Detailed** from the drop-down menus for the relevant components. Click **Update Trace Levels** to apply the changes.
3. Recreate the problem in your deployment or wait until the problem occurs again.
4. Return to the Log Collection tool and collect logs for the appropriate date and time interval, during which detailed trace level was selected. For example, if you set the trace level to detailed on 01/27/2014 at 09:00, you can collect detailed logs for intervals after that date and time.
5. When you have finished debugging the problem, reset the trace level to **Normal**.

To collect log files:

1. In **Unified CCE Administration**, choose **Overview** > **Infrastructure Settings** > **Log Collection**.
2. Check each component for which you want to collect logs, or check **Select All**.
3. Click the **calendar** icon to select a **Start Time** and **End Time** for log collection. Select a date and time from the calendar, and then click anywhere outside the calendar to save your selection.
4. Click **Collect Logs**.

   The new log collection appears in the list with an **in progress** icon in the Status column. When the log collection is complete, its **download** and **delete** icons are enabled automatically.

Note If errors are encountered during log collection, the **Status** column shows an **error** icon. Hover over the icon to view the tooltip which explains the error. If the Unified CCE Administration service restarts during log collection, a **cancelled** icon appears in the Status column. You can delete log collections that have errors or have been cancelled; you cannot download these collections.

5. Click the **download** icon to download the log zip file.

To delete a stored log collection, click the **delete** icon for that collection in the list.

Command Execution Pane

The Command Execution Pane provides a user interface in the Unified CCE Administration. This pane allows System Administrators to run REST API calls to Unified CVP, Unified CVP Reporting, and Virtualized Voice Browser.

Caution Use this pane to configure certain parameters in Unified CVP, Unified CVP Reporting, and Virtualized Voice Browser, for which no user interface is available in the Unified CCE Administration.

For example:

- To configure DNIS in CVP

  For API details, see the *Unified CVP API Developer Guide* at https://developer.cisco.com/site/customer-voice-portal/documents/rest-api/.

- To configure Customer Virtual Assistant (CVA) feature in VVB 12.5(1), while keeping the Unified CCE Controller in ICM12.0(1)_ES 37 (or higher), in case of multi-stage upgrade.

Before you begin

If you do not have CA certificates, import self-signed certificates of CVP Call Server and Virtualized Voice Browser (VVB) into the AW machines. For more information, see and Import VVB Self-Signed Certificate into AW Machines.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Infrastructure Settings** > **Command Execution Pane**.

Step 2 Complete the following parameters.

Field	Description
Machine Type	Choose the machine type. Valid values are: • Unified CVP • Unified CVP Reporting • Virtualized Voice Browser
Site	Choose the site. You can run the REST API call on the Main site or the Remote site machines. Default is All Sites when a Machine Type is selected.
Host Name	Choose a Host Name or multiple Host Names. Host Names are displayed based on the selected Machine Type and Site.
Method	Choose the HTTP method. Valid values are: • GET • POST • PUT • DELETE Default is GET.
Path	Enter the relative URI of the API. Based on the Machine Type you select, most frequently used APIs are displayed as auto suggestions. For example, when the Machine Type is **Unified CVP**, the path displayed is `cvp-orm/rest/cvpconfig/properties`. For more information about APIs, refer to the respective CCE Component documentation.
Request Body	Enter the request data in JSON or XML format. Mandatory if the Method is POST or PUT.
Response Type	Choose the Response Type as JSON or XML. Default is JSON. **Note** Response Type is only applicable for Success result.

Step 3 Click **Execute**.

The window displays the Success or Failure response.

Note The **RESET** button resets all the fields on the page to its default value.

User Setup

Manage Agents

Agents

Agents respond to contacts from customers. These contact requests are often phone calls, but can also be chat requests or emails.

You can configure the types of contacts that are routed to an agent. For example, if an agent is a member of a skill group that is set up for the Cisco_Voice routing domain only, that agent is a voice agent for that skill group. If an agent is a member of a skill group that is set up for a nonvoice routing domain, that agent is a multichannel agent for that skill group.

Agents can be located at a contact center site or designated as mobile agents who work elsewhere—perhaps from a home office. Setting up mobile agents is documented in the *Cisco Packaged Contact Center Enterprise Features Guide* , at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Agents can be assigned to skill groups and to one team. Teams are organizational units that reflect the reporting structure in a contact center. They can also be assigned attributes that indicate their proficiency—perhaps expertise in a certain language or technology.

Agents work from an agent desktop. Each agent is associated with one Desk Settings, either the current default desk settings or another desk settings. Desk settings are a set of permissions or characteristics that control the features agents can see and use while they are interacting with customers.

You can indicate that an agent is a supervisor. An agent with supervisor status can oversee multiple teams, can view reports that monitor activities of the agents on those teams, and can join and participate in agent/customer calls. Supervisors work from a supervisor desktop.

In **Unified CCE Administration**, choose **Users** > **Agents** to view the Agent list. the administrators can see and maintain all agents. Supervisors see a list of agents who are on teams they supervise.

Related Topics

Add and Maintain Agents, on page 80
Add an Agent by Copying an Existing Agent Record, on page 84
Edit Description, Desk Settings, and Teams for Multiple Agents, on page 88
Add Supervisor Status to an Agent, on page 91
Attributes, on page 109
Desk Settings, on page 172
Roles, on page 91
Skill Groups, on page 106
Teams, on page 99

Add and Maintain Agents

This procedure explains how to add an agent. For information on maintaining agents, see Update Objects, on page 4 and Delete Objects, on page 7.

You can add agents one at a time from the **Agents** page , using this procedure. You can also do the following:

- Create a new agent by copying an existing agent record (see Add an Agent by Copying an Existing Agent Record, on page 84).
- Run bulk jobs to add or edit multiple agent records (see Manage Bulk Jobs, on page 227).
- Edit the skill group membership for multiple agents at once (see Edit Skill Group Membership for Multiple Agents, on page 87).
- Edit descriptions, desk settings, and teams for multiple agents at once (see Edit Description, Desk Settings, and Teams for Multiple Agents, on page 88).

Procedure

Step 1 In **Unified CCE Administration**, choose **Users** > **Agents**.

Step 2 Click **New** to open the **New Agent** page.
This page has **General**, **Description**, **Attributes**, **Skill Groups**, **Supervised Teams** , and **Email & Chat** tabs. You cannot save the agent until you have entered all the required fields on the **General** tab. You can complete other tabs as needed and in any order.

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

Field	Required?	Description
Enable SSO	no	Indicates whether the agent is set for single sign-on (SSO). When SSO is enabled, the agent uses Active Directory or other SSO credentials to sign into the agent desktop and other tools. You can check this check box to enable SSO for this agent if SSO is set globally to mixed mode. You cannot edit this setting if SSO is enabled or disabled globally. If SSO is enabled globally, saving the agent's new or updated record enables SSO for the agent.
Login Enabled	no	Checked by default. Uncheck the check box only if you do not want this agent to be able to sign in.

Field	Required?	Description
Is Supervisor	no	Check to configure this agent as a Supervisor. **Note** • When you check this check box, a user account is created in Cisco Unified Intelligence Center with the supervisor's username and domain name. If the username and domain name exists in Unified Intelligence Center, the user account and supervisor's record is synchronized to have same username and domain name. • For an existing supervisor's record, if you uncheck this check box, the corresponding user account is deleted from Unified Intelligence Center.
Support Email & Chat	no	This check box appears only when ECE is configured for a peripheral set or a data center. By default, it is not checked.
Username	yes	Enter a unique username for the Agent. Enter up to 255 ASCII characters as the username for this agent. The login name supports the use of all characters from 33 to 126 in the ASCII character set, except for the following: double quotation mark ("), forward slash (/), backward slash (\), square brackets ([ ]), colon (:), semicolon (;), pipe (|), equal to (=), comma (,), plus sign (+), asterisk (*), question mark (?), angle brackets (< >), hash (#), percent (%), and SPACE. For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username. For supervisors who are not enabled for single sign-on (SSO), the Active Directory username must be in the user@domain format. **Remember** An agent who is designated as a supervisor signs in to Unified CCE Administration with this username. **Note** Ensure that Agent ID (Peripheral number) and agent Login name is unique for each user.
First Name	yes	See Character Sets.
Last Name	yes	See Character Sets.
Agent ID	-	Enter a unique string of up to 11 digits. If you leave this field blank, Packaged CCE automatically generates a 7-digit agent ID, which you can later edit. The agent uses the Agent ID to sign in to Cisco Finesse.
Description	no	Enter a description of the agent. See Character Sets.

Field	Required?	Description
Desk Settings	-	The **Desk Settings** field defaults to show the current system-default. (See Main Site, on page 212.) To change it, click the **magnifying glass** icon to display the **Select Desk Settings** list where you can select a different desk setting.
Department	yes (for departmental administrators)	A departmental administrator must select one department from the pop-up list to associate with this agent. The list shows all administrator's departments. A global administrator can retain the default value for this field, which sets the agent as global (belonging to no departments), or can select a department for this agent. See Departments, on page 119 for more information about associating agents with departments.
Site	-	The **Site** field displays Main by default for Packaged CCE 2000 Agents deployment. For Packaged CCE 4000 Agents and 12000 Agents deployments, **Site** is a mandatory field and has no default value. To add a site: **a.** Click the **magnifying glass** icon to display the list of sites. **b.** Select the required site.
Peripheral Set	yes	This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set. To add a peripheral set: **a.** Click the **magnifying glass** icon to display the list of peripheral sets configured for the selected **Site**. **b.** Select the required peripheral set.
Team	no	The **Team** field defaults to *None*. To change the setting, click the **magnifying glass** icon to display the **Select Team** list and select a team. Only the teams associated to the selected site display. If the agent is associated with a department, you see global teams and teams that are associated with that department in the list. If the agent is a global agent, you see only global teams in the list. **Note** When you add a team to an agent, the same agent is added to the corresponding collection in Unified Intelligence Center.
Set Password	no	If single sign-on is not enabled, this setting is checked by default. Uncheck the check box if you do not want to create a password for this agent. If single sign-on is enabled, the password settings on the **General** tab are disabled.

Field	Required?	Description
Enter Password	no	Enter and reenter a maximum of 256 ASCII characters to establish and confirm a password for this agent. Password is case-sensitive. The default *Minimum Password Length* is set in system settings. (See Global, on page 210.) For a supervisor, the password must be the supervisor's Active Directory password. **Tip** An agent who is designated as a supervisor signs in to Unified CCE Administration with this password.
Re-enter Password	no	—

Step 4 Complete the **Attributes** tab:

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

Click the + icon to open a pop-up 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) From the **Value** drop-down list, choose the attribute value as appropriate for this agent.

Step 5 Complete the **Skill Groups** tab:

This tab shows the skill group membership for this agent.

a) Click the + icon to open the **Add Skill Groups** pop-up. You can view only the skill groups associated to the selected site.Click the skill groups you want to add for this agent or supervisor.

Note You can view only the skill groups associated to the selected site in 2000 Agents deployment.

You can view only the skill groups associated to the selected site and peripheral set in 4000 Agents and 12000 Agents deployment.

b) Select the default skill group for the agent from the **Default Skill Group** drop-down list.

Step 6 Complete the **Supervised Teams** tab, if **Is Supervisor** is checked.

To select a team, click the + icon to display the **Add Supervised Teams** list, and click the row to select a team.

Note
- You can view only the teams that are associated to the selected site in 2000 Agents deployment.
- You can view only the teams that are associated to the selected site and peripheral set in 4000 Agents and 12000 Agents deployment.
- If the supervisor is associated with a department, you see only teams associated with that department in the list. If the supervisor is a global supervisor, you see all global and departmental teams in the list.
- When you associate teams for a supervisor, the same teams (collections in Unified Intelligence Center) are also associated to the corresponding user account (with Supervisor permission) in Unified Intelligence Center.

Step 7 Complete the following fields in the **Enable Email & Chat** tab if Cloud Connect is added and registered or ECE is configured.

Field	Required?	Description
Screen Name	yes	The screen name of the ECE-enabled agent. The screen name must be at least 1 character and no more than 30 characters. The following characters can be used in screen names: Uppercase and lowercase alpha numeric characters (A-Z, a-z, 0-9); at sign (@); space ( ); colon (:); period (.); underscore (_); hyphen (-); ampersand (&); and all the characters above ASCII codeset 128. This field is required if Support Email & Chat is checked.
Email Address	no	The email address of the ECE-enabled agent. Maximum length is 50 characters. Email address is mandatory when this checkbox is selected.

Step 8 Complete the **Email & Chat** tab. Enter the **Screen Name** and **Email Address**. Click **Save**.

Note The screen name of the ECE-enabled agent. Maximum length is 32 characters.Valid characters are period (.), underscore (_), and alphanumeric. The first character must be alphanumeric.

Note This tab is available only if ECE is configured for a peripheral set or a data center.

Step 9 Click **Save** to return to the List window, where a message confirms the successful creation of the agent.

Caution You cannot add a new agent in the following conditions:

- Out of Compliance expiry: The system is operating with an insufficient number of licenses and the system is in enforcement mode.
- Authorization expiry: The system has not communicated with **Cisco Smart Software Manager** or satellite for 90 days and the system has not automatically renewed the entitlement authorizations.
- Evaluation expiry: The license evaluation period has expired.

Add an Agent by Copying an Existing Agent Record

You can create a new agent by copying an existing agent record.

The following fields are copied to the new agent record:

- Department
- Description
- Desk settings
- Team
- Attributes
- Skill Groups
- Default Skill Group
- Site

All other fields are either cleared or set to the default value.

Procedure

Step 1 In **Unified CCE Administration**, choose **Users** > **Agents**.

Step 2 Click the agent you want to copy, and then click the **Copy** button in the **Edit Agent** page.
The **New Agent** page opens.

Step 3 Hover over the row for that agent, and click the **copy** icon that appears at the end of the row.

Step 4 Review the fields on the **General**, **Attributes**, and **Skill Groups** tabs that were copied from the original agent record, and make any necessary changes. Enter information for the fields that were not copied.

Step 5 If the new agent is a supervisor, complete the fields on the **Supervisor** tab.

Step 6 Click **Save** to return to the List window, where a message confirms the successful creation of the agent.

Note If the new agent is a supervisor, a user account is created in Cisco Unified Intelligence Center with the supervisor's username and domain name.

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 peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Enter one or more team names separated by spaces. (Team is an OR search--the agent or supervisor must be a member of one of the teams.)
- Enter one or more attribute names separated by spaces. (Attributes is an AND search--the agent or supervisor must have all attributes.)
- Enter one or more skill group names separated by spaces. (Skill Groups is an AND search.)
- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.
- Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Departments is an OR search.)

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

Search by site is available only when remote sites are configured.

Manage Agent Expertise

There are two ways that agents can be categorized such that calls are sent to them based on their experience and their expertise in handling specific types of customer concerns.

- You can add an agent to one or more skill groups. For example, agents who work on fulfilling orders might be added to a *Customer Service* or a *Tracking Orders* skill group.
- You can assign one or more attributes to an agent. For example, an agent who speaks fluent Spanish might be assigned an attribute of *Spanish*.

Agent Reskilling

Supervisors can reskill agents who are on teams that they supervise. This procedure explains how to reskill a single agent. For information on reskilling multiple agents at once, see Edit Skill Group Membership for Multiple Agents, on page 87.

Note If you remove an agent from the agent's default skill group, the agent's default skill group is changed to the system defined default skill group.

Procedure

Step 1 In **Unified CCE Administration Manage**, choose **Users** > **Agents** to view the Agents list.

Step 2 Click the agent you want to reskill.

Step 3 Click the **Skill Groups** tab.

Step 4 To add a skill group, click the **magnifying glass** icon to open the pop-up list of skill groups. Work in the pop-up window to add skill groups to the agent.

Step 5 To remove a skill group, click the skill group's **x** icon in the **List of Skill Groups** section of the **Skill Groups** tab.

Step 6 Click **Save**.

Edit Skill Group Membership for Multiple Agents

Using the Agent tool, you can edit skill group membership for multiple agents at once.

In Packaged CCE deployments only, the agents must all belong to the same site and same department, or all be global agents. The **Edit** button disables if you select:

- Agents from multiple sites or multiple departments.
- A mix of global and departmental agents.
- A mix of agents on main site and remote site.

The agents must all belong to the same department or all be global agents. The **Edit** button is disabled if you select agents from multiple departments, or if you select a mix of global and departmental agents.

If you remove an agent from the agent's default skill group, the agent's default skill group is changed to the system defined default skill group.

Tip Use the **Search** field to find the agents whose skill group membership you want to edit. For example, you could find agents belonging to a particular department, team, or skill group, or with certain attributes. (See Search for Agents, on page 85.)

Procedure

Step 1 In **Unified CCE Administration**, choose **Users** > **Agents**.

Step 2 Check the check box for each agent whose skill group membership you want to edit.

To select all agents in a list, check the **select/deselect all** check box in the list header. (The check box is enabled for *select all* only when the number of agents in the list is less than or equal to 50.)

The total number of selected agents appears above the agent list. To uncheck all agents, click the **select/deselect all** check box. (The check box is enabled for *deselect all* when you check one or more agents in the list, regardless of the number of agents in the list.)

Step 3 Click **Edit** > **Skill Groups**.

The **Edit Skill Groups** dialog opens with a list of skill groups.

The **# of Selected Agents** column indicates how many of the selected agents currently belong to each skill group.

In Packaged CCE deployments only, if you select agents from a specific department and a site, global skill groups on that site, and skill groups for that department and site appear in the list. If you have selected global agents from a specific site, all global and departmental skill groups on that site appear in the list.

Step 4 In the **Action** column, click the **+** icon for each skill group to which you want to add the selected agents. Click the **x** icon for each skill group from which you want to remove the selected agents.

Note If all selected agents belong to a skill group, only the **x** icon appears for that skill group. If none of the selected agents belong to a skill group, only the **+** icon appears for that skill group.

The total number of skill groups that you are adding and removing appears at the bottom of the dialog.

Step 5 To undo a skill group membership change, click the **Undo Add** icon in the **Action** column for that skill group.

Step 6 Click **Save**, and then click **Yes** to confirm the changes.

Edit Description, Desk Settings, and Teams for Multiple Agents

Using the Agent tool, you can edit the description, desk settings assignment, and team membership for multiple agents at once.

The agents must all belong to the same site and same department, or all be global agents. The **Edit** button disables if you select:

- Agents from multiple sites or multiple departments.
- A mix of global and departmental agents.
- A mix of agents on main site and remote site.

Tip Use the **Search** field to find the agents whose settings you want to edit. For example, you could find agents belonging to a particular department, team, or skill group, or with certain attributes. (See Search for Agents, on page 85.)

Procedure

Step 1 In **Unified CCE Administration**, choose **Users** > **Agents**.

Step 2 Check the check box for each agent whose description, desk settings, and team membership you want to edit.

To select all agents in a list, check the **select/deselect all** check box in the list header. (The check box is enabled for *select all* only when the number of agents in the list is less than or equal to 50.)

The total number of selected agents appears above the agent list. To clear all agents, check the **select/deselect all** check box. (The check box is enabled for *deselect all* when you check one or more agents in the list, regardless of the number of agents in the list.)

Step 3 Click **Edit** > **General**.

The **Edit General Details** pop-up windows opens.

Step 4 To change the description for all selected agents, check the **Description** check box and enter the description in the text field.

Step 5 To assign desk settings to all selected agents:

a) Check the **Desk Settings** check box.

b) Click the **magnifying glass** icon to display the **Select Desk Settings** list, and then select the desk setting.

Step 6 To assign all selected agents to a team:

a) Check the **Team** check box.

b) Click the **magnifying glass** icon to display the **Select Teams** list, and then select the team.

Step 7 Click **Save**, and then click **Yes** to confirm the changes.

Manage Supervisors

You can configure agents to have supervisor status.

Supervisors with Single Sign-on (SSO) enabled, use their SSO credentials to sign in to Unified CCE Administration.

Supervisors with Single Sign-on (SSO) disabled, use their Unified ICM credentials to sign in to Unified CCE Administration.

With Supervisor status, agents can perform the following tasks:

- Supervise multiple teams and can be both a supervisor and a member of a team.
- Generate reports and view data for the teams they supervise and the agents on those teams.
- Use a supervisor desktop to barge-in, intercept, silently monitor, and log out agents.
- Join an agent or customer call to assist on a consultative or emergency basis. The agent's ability to request supervisor assistance is a setting on the Desk Settings.
- Change the attributes, and skill groups of agents who are on teams they supervise. Supervisors can also change the passwords for agents who do not have single sign-on enabled.

To configure supervisors in **Unified CCE Administration**, choose **Users** > **Agents**. Click an agent and check the **Is Supervisor** check box on the **General** tab.

Supervisor Access and Permissions

Supervisors can access the following tools:

Tool	Permissions
Agents	On the Agent List page, supervisors can see and edit settings for the agents that they supervise. • **General** tab: Supervisors can edit the password for agents who do not have single sign-on enabled. Other fields are read-only. After changing the agent's password, • The agent can sign in to Cisco Finesse only after 30 minutes, or • Restart Unified Intelligence Center Reporting Service and then the agent can sign in to Cisco Finesse. • **Attributes** tab: Supervisors can add, modify, and remove attributes for agents on teams they supervise. • **Skill Groups** tab: Supervisors can add and remove the agent's membership in skill groups and can change the agent's default skill group. • **Supervised Teams** tab: Read-only for supervisors. Supervisors can also change skill group or attribute assignments for up to 50 agents at once by selecting the agents on the Agent List page, and then clicking **Edit > Skill Groups** or **Edit > Attributes**. **Note** If a supervisor attempts to make numerous membership changes at once (in excess of 3500 in a single save), the system alerts the supervisor of attempting too many changes in a single operation.
Attributes	On the Attributes List window, supervisors can see and edit agent attribute assignments. Supervisors cannot add or delete attributes. • General tab: Fields are read-only. • Agents tab: Supervisors can add and remove attribute assignments for agents that they supervise.
Precision Queues	Read-only.
Skill Groups	On the Skill Group List page, supervisors can see and edit membership for skill groups. Supervisors cannot add or delete skill groups. • **General** tab: Fields are read-only. • **Members** tab: Supervisors can add and remove skill groups for agents that they supervise.
Teams	Read-only.
Business Hours	On the Business Hours page, supervisors can see and edit all the fields for business hours. Supervisors cannot add or delete business hours.

Add Supervisor Status to an Agent

This procedure explains how to create a supervisor. For information on maintaining supervisors, see Update Objects, on page 4 and Delete Objects, on page 7.

Remember The agent to whom you are adding supervisor status must already exist in Active Directory.

In **Unified CCE Administration**,choose **Users** > **Agents**.

Procedure

Step 1 Create a new agent or edit an existing agent. See Add and Maintain Agents, on page 80.

Step 2 Check **Is Supervisor** to configure this agent as a Supervisor.

Note
- When you check this check box, a user account is created in Cisco Unified Intelligence Center with the supervisor's username and domain name. If the username and domain name exists in Unified Intelligence Center, the user account and supervisor's record is synchronized to have same username and domain name.
- For an existing supervisor's record in Packaged CCE, if you uncheck this check box, the corresponding user account is deleted from Unified Intelligence Center.

Step 3 Click the **Supervised Teams** tab.

Step 4 Select the teams for this supervisor:

a) Click **Add** next to **List of Supervised Teams** to open **Add Supervised Teams**.
b) Click the team name to add the team.

Note When you associate teams for a supervisor, the same teams (collections in Unified Intelligence Center) are also associated to the corresponding user account (with Supervisor permission) in Unified Intelligence Center.

Step 5 Click **Save** to create the supervisor.

Manage Roles

Roles

Roles specify which features and subfeatures an administrator can see and use. An administrator can be assigned to a built-in role or to a custom role. (An administrator who has no role cannot sign in.)

In **Unified CCE Administration**, choose **Users** > **Roles** to view the list of roles currently configured.

Features and subfeatures access for roles are defined by check boxes. You cannot alter the features and subfeatures access for built-in roles (all allowed features and subfeatures are checked). But, you can create custom roles to define customized sets of features and subfeatures access.

Note Role changes can take up to 30 minutes to take effect.

Built-In Roles

On the **Roles** page, click the built-in role to view the features and subfeatures associated with it.

Built-In Role Name	Associated Features and Subfeatures

AgentAdmin	The administrators assigned with this role can access the following features and subfeatures.
	• Agents:
	  • Manage Agents
	  • Manage Agent Attributes
	  • Reskill Agents
	• Outbound Campaigns:
	  • Campaign Status & Schedule
	  • Campaign Contact
	• Desktop Settings:
	  • Desktop Layout
	  • Phonebook
	  • Reason Codes
	  • Workflow

ScriptAdmin	The administrators assigned with this role can access the Agent feature and Call Settings feature, and its subfeatures.
ConfigAdmin	The administrators assigned with this role can access all the features and subfeatures except for the Access feature and its subfeatures.
SystemAdmin	The administrators assigned with this role can access all the features and subfeatures.

Related Topics

Add and Maintain Custom Roles, on page 92

Add and Maintain Custom Roles

To add, edit, or delete custom roles, an administrator must have the SystemAdmin role.

This procedure explains how to add a role. For information on maintaining roles, see Update Objects, on page 4 and Delete Objects, on page 7.

Procedure

Step 1 In **Unified CCE Administration**, choose **Users** > **Roles**.
On the **Roles** page, you can view all the roles currently configured.

Step 2 Click **New** to open the **New Role** page.

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

Field	Required?	Description
Name	Yes	Enter a unique name for the role, using a maximum of 32 characters.
Description	No	Enter a maximum of 255 characters to describe the role. See Character Sets.
Features and Subfeatures Access fields	No	When you create a new (custom) role, check the check box corresponding to the features and subfeatures that you want administrators with this role to be able to see and use. Checking a check box corresponding to a feature checks all the subfeatures' check boxes in that feature. You can uncheck individual subfeatures within a feature. For example, you can check the Organization feature and then uncheck Precision Queues and Skill Groups subfeatures. **Note** You cannot add Access tools (Administrators, Departments, Roles) to a custom role.

Step 4 Continue to the **Administrators** tab to add administrators to the role.

Step 5 Click the + icon to open the **Add Administrators** pop-up window.

The row for each administrator has two columns: a column with Administrator's Username and a column with Administrator's Domain.

Clicking an administrator who already has a role removes that role and reassigns this role.

On the **Overview** page, the administrator can view only the cards and its access tools associated with the assigned role.

Step 6 Click **Save** to return to the list of roles, where a message confirms the successful creation of the role.

Manage Administrators

The Packaged CCE deployment of Unified CCE Administration offers extensive flexibility in the configuration of administrator users and in ways to limit their system access.

Administrator access is controlled by the **Roles** tool available from the **User Settings** page and **Departments** tool available from the **Organization** menu. Only administrators with the SystemAdmin role can access these pages.

Note Administrator password and role changes can take up to 30 minutes to take effect.

Note If the system administrator is assigned to "None" (no role), then that administrator has access all the tools in the Configuration Manager.

Add and Maintain Administrators

This procedure explains how to add an administrator. For information on maintaining administrators, see Update Objects, on page 4 and Delete Objects, on page 7.

To add, edit, or delete administrators, an administrator must have the SystemAdmin role. Administrators cannot add, update, or delete themselves.

Before you begin

The administrators you create are added to the domain security group and CCE database based on their role, if `ADSecurityGroupUpdate` registry key is set to 1. If `ADSecurityGroupUpdate` registry key is set to 0 (default setting), the administrators are added only to the CCE database based on their role.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Users** > **Administrators**.

This displays a list of administrators who are currently configured.

Step 2 Click **New** to open the **New Administrator** window.

Step 3 Complete the following fields:

Field	Required?	Description
Domain	no	From the drop-down menu, select the domain for this administrator.
Username	yes	Enter a unique name for the administrator, using a maximum of 64 characters. The account must already exist in Active Directory under the selected domain.
Description	no	Enter a maximum of 255 characters to describe the role. See Character Sets for details on valid characters for this field.

Field	Required?	Description
Role	no	*ConfigAdmin* is the default role for a new administrator. Click the **magnifying glass** icon to open the **List of Roles** pop-up window. Select a role for this administrator. On the **Overview** page, the administrator can view only the cards and its access tools associated with the assigned role. For more infromation see the topic
Access to All Departments	no	This check box defaults to checked. You cannot uncheck it for the *SystemAdmin* role—SystemAdmins are always Global administrators. For all other roles, you can leave the check box checked to configure the new administrator as a Global administrator. Or you can uncheck the check box to configure the administrator as a Department Administrator and then: • Click the + icon to open the **Add Departments** pop-up window. • Click one or more departments to select them; then close the popup window. The administrator is now a Department administrator who is associated with those departments. • Click the **x** icon to remove a department. **Note** Department Administrator will have read-only access to non-departmental entities such as SIP Server Group, Media Routing Domain, Routing Pattern, and so on, even if the associated role grants full access.

Step 4 Click **Save** to return to the list, where a message confirms the successful creation of the administrator.

Related Topics

Changing Authorization Modes of Administrators , on page 98
Administrators and System Access, on page 95
Departments, on page 119
Roles, on page 91

Administrators and System Access

Administrators' access to the system can be restricted by their roles, the departments to which they are assigned, and whether they have full or read-only permission.

An administrator must have a role, which specifies which cards and access tools that an administrator sees on the **Overview** page.

Packaged CCE offers the option to create departments. A contact center for a university might have a department for each academic area, a department for admissions, a department for alumni, and so forth. An administrator

can be associated with one or more departments or can be a global administrator who is assigned to no departments and who therefore has access to all departments. Departmental administrators can add and edit objects only for the departments they administer.

An administrator's role and department associations are configured when the administrator is created. A SystemAdmin can change them.

Note If user's Use logon name (pre-Windows 2000) changes in Active Directory, you must update the same in Packaged CCE. Choose **Unified CCE Administration** > **Users** > **Administrators**. Select the user to open the details and click **Save**.

Related Topics

Roles, on page 91
Departments, on page 119

Limit Administrator Access

Limit Administrator Access by Departments

Packaged CCE allows you to create departments and to associate an object with one department. For example, a university might have department for Admissions, Billing, and each academic area.

The add/edit pages for those objects have a Department field. If you do not want an object to have a department association, you have two options:

- Do not create departments.
- Create departments, but select *Global* from the Department drop-down menu to give the object "global" status.

In the table below, Skill Group One is associated with the Admissions department. Skill Group Two is associated with the History department. Skill Group Three is global and belongs to no department.

Table 15: Object and Departments

Department	Object
Admissions	Skill Group One
History	Skill Group Two
Global	Skill Group Three

When you create or edit an administrator, you can either check **Access to All Departments**, which gives an administrator "global" access to all departments, or associate the administrator with one or more departments. To establish a department association for an administrator, click **Add New** next to the **List of Allowed Departments** and select one or multiple departments.

Note An administrator with the SystemAdmin role cannot be a departmental administrator.

In the following table, Administrator One can work with objects in the Admissions department. Administrator Two can work with objects in the History department. Administrator Three is a global administrator and can work with all objects in all departments.

Table 16: Administrators and Departments

Department	Administrator
Admissions	Administrator One
History	Administrator Two
Global	Administrator Three

Limit Administrator Access by Role and Permissions

An administrator must be assigned a role to be allowed to sign in to the Unified CCE Administration.

Permissions defined in the following table indicate which tools an administrator can view, add, edit, or delete, unless restricted by departmental association.

Table 17: Administrator Tools and Permissions

Administrator	Tool	Permissions
Administrator One	Agent Tools	• Full access to Agent Tools • View, add, edit, and delete Skill Group One • Add Admissions Department agents to Skill Group One • Add global agents to Skill Group One • View Skill Group Three
Administrator Two	Agent Tools	• Full access to Agent Tools • View, add, edit, and delete Skill Group Two • Add History Department agents to Skill Group Two • Add global agents to Skill Group Two • View Skill Group Three
Administrator Three	Script and Call Tools	• Full access to Script and Call Tools • Full access to agents and Skill Groups from all departments • Full access to global agents and Skill Groups

Changing Authorization Modes of Administrators

When you provide permissions to a user (account):

The registry settings in the local AW machine **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Cisco Systems Inc** > **ICM** > **<instance>** > **AW** with the key ADSecurityGroupUpdate decides whether a user will be added to the domain Config and Setup Security Groups.

Default Key Value

The default value of the **ADSecurityGroupUpdate** key is 0 which means that the AW is in local authorization mode. If the user is added using the Administrator Gadget or the API with **pre-defined** or **custom roles**, the user is not added to the corresponding domain security groups. The user is added to the database with the corresponding roles.

If you want to use the configuration manager tool, then you have to provide a user with the Config permissions, add the user to the `UcceConfig` local security group manually.

To provide a user the Setup permissions, add the user to the `UcceConfig` and local administrator security groups of the AW machine manually.

Key value Set to 1

If the value of the `ADSecurityGroupUpdate` key is set to 1, the AW machine is in the domain authorization mode. If the user is added using the Administrator Gadget or the API with **pre-defined** or , the user is added to the corresponding domain security group. The user is added to the database with the corresponding roles. There is no need to manually add the user to the local groups of the AW machine.

Move to Local Authorization Mode

To move to Local Authorization mode from domain authorization you have to change the registry `ADSecurityGroupUpdate` from 1 to 0.

All the existing users which are available in domain Config and Setup security groups under instance OU must be manually moved to `UcceConfig` local group of all AW machine except Admin Client machine. All the users in the domain setup security group has to be added to the local Administrators group of all AW machine except Admin Client machine.

Remove the users from domain Config and Setup security group under instance OU.

Move to Domain Authorization Mode

To move to domain authorization mode from local authorization mode you have to change the registry `ADSecurityGroupUpdate` from 0 to 1.

All the users in local `UcceConfig` group of all the AW except Admin Client has to be added manually to the domain Config security group.

Remove all users from local `UcceConfig` group.

Identify the system admininstrator role users from the Administrator Gadget and move those users from local Administrators group of all AW (except Admin Client) to the domain setup security group. Remove those users from local Administrators group.

Organization Setup

Manage Teams

Teams

You can create teams to associate a set of agents with supervisors. Supervisors can run reports on the team and receive Supervisor Assist requests from the team members.

Note Supervisor Assist must be indicated in the Desk Settings tool and must be supported by the agent desktop.

Agent cannot be a member of more than one team.

After you create a team with agents and/or supervisors, you can assign resources such as custom desktop layout, phone books, reasons (not ready, sign out, and wrap-up), and workflow to the team.

The desktop layout, phone books, and workflow resources are preconfigured in **Desktop** > **Resources**. The reasons (not ready, sign out, and wrap-up) are preconfigured in **Desktop** > **Reason Labels**.

Administrators can see and maintain teams .

Supervisors have display-only access to the Teams tool.

To configure teams, navigate to **Unified CCE Administration** > **Overview** > **Organization Setup** > **Teams**, or choose **Organization** > **Teams** from the left navigation.

Related Topics

Add and Maintain Teams , on page 99
Agents, on page 79
Manage Supervisors, on page 89
Add and Maintain Desk Settings, on page 172

Add and Maintain Teams

Procedure

Step 1 In **Unified CCE Administration** , choose **Organization** > **Teams** from the left navigation.

Step 2 Click **New** to open the **New Team** page.

Step 3 Complete the following fields on the **Basic Details** tab:

Field	Required?	Description
Name	Yes	Enter up to 32 alphanumeric characters.
Description	No	Enter up to 255 characters to describe the team. See Character Sets.

Field	Required?	Description
Site	-	The **Site** field displays Main by default for Packaged CCE 2000 Agents deployment type. To add a different site: **a.** Click the **magnifying glass** icon to display the list of sites with Agent PG configured. **b.** Select the required site.
Peripheral Set	Yes	**Note** Before you add a **Peripheral Set**, you must select a **Site**. The **Peripheral Set** field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set. To select a peripheral set: **a.** Click the **magnifying glass** icon to display the list of peripheral sets that are configured for the selected **Site**. **b.** Select the applicable peripheral set.
Supervisor DN (Dialed Number)	No	Click the **magnifying glass** icon to display the **Select Supervisor Script Dialed Number** list. The list includes all dialed numbers with a routing type of **Internal Voice**. Click a row to select a dialed number for the supervisor assistance and close the list.

Step 4 Click the **Team Members** tab.

a) Click the + icon to open the **Add Agents** popup window.
The agents associated to the selected site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) appear. If the team is associated with a department, you see only agents associated with that department in the list. If the team is a global team, you see both global and departmental agents in the list.

The "i" icon indicates that the agent is a member of a team. Hover over the icon to see the name of that team. Clicking an agent who already has a team removes that agent from that team and reassigns the agent to this team.

b) Click one or more rows to select agents. The agents are now in **List of Agents**.

Note When you add or remove agents to a team, the same information is updated in the corresponding collection in Unified Intelligence Center.

Step 5 Click the **Supervisors** tab.

a) Click the + icon to add supervisors to the team. The supervisors associated to the selected site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) appear in the **Add Supervisors** popup window. If the team is associated with a department, both global supervisors and supervisors associated with that department appear in the list. If the team is a global team, only global supervisors appear in the list.
b) Click one or more rows to select the supervisors. The supervisors are now in **List of Supervisors**.

Note When you add Supervisors to a team, the same Supervisors (user accounts in Unified Intelligence Center) are added (with Supervisor permission) to the corresponding collection in Unified Intelligence Center.

Step 6 Click the **Team Resources** tab.

Note Before you configure **Team Resources**, add Agent(s) or Supervisor(s) to the team.

This tab includes the following subtabs to configure the team resources:

Subtab	Description
Desktop Layout	To customize the site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) specific desktop layout for the team: **a.** Check the **Customize** check box. You can now edit the **Desktop Layout** section. This section includes default desktop layout XML that is defined in **Desktop** > **Resources** > **Desktop Layout**. **b.** Edit the XML. To revert the changes, click **Revert Changes**. **Note** • If you clear the **Customize** check box without saving the changes, the system reverts to the default desktop layout. • To add the Live Data report gadgets to the desktop layout, seeAdd Live Data Reports to Team Layout, on page 103.
Phone Books	To assign phone books to the team: **a.** Click the + icon. The **Add Phone Books** pop-up window opens with a list of phone books that are configured for the site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments). The phone books are configured for **Teams** in **Desktop** > **Resources**. **b.** Select one or more phone books from the list. Use the Sort a List and Search a List features to navigate the list. The selected phone books are highlighted in the pop-up window, and appear in **List of Phone Books**. You can click the **Name** header to sort the phone books. To unassign a phone book from the team, click 'x' next to the phone book in **List of Phone Books**.

Not Ready Reasons	To assign not ready reasons to the team: **a.** Click the + icon. The **Add Not Ready Reasons** pop-up window opens with a list of not ready reasons. The reasons are configured as **Team Specific** in **Desktop** > **Reason Labels** > **Phone Books**. **b.** Select one or more reasons from the list. Use the Sort a List and Search a List features to navigate the list. **Note** The search field does not allow searching the list by code. The selected reasons are highlighted in the popup window, and appear in **List of Not Ready Reasons**. You can click the **Label** header to sort the reasons. To unassign a not ready reason from the team, click 'x' next to the reason in **List of Not Ready Reasons**.
Sign Out Reasons	To assign sign out reasons to the team: **a.** Click the + icon. The **Add Sign Out Reasons** popup window opens with a list of sign out reasons. The reasons are configured as **Team Specific** in **Desktop** > **Reason Labels**. **b.** Select one or more reasons from the list. Use the Sort a List and Search a List features to navigate the list. **Note** You cannot search the list by code in the pop-up window. The selected reasons are highlighted in the pop-up window, and appear in **List of Sign Out Reasons**. You can click the **Label** header to sort the reasons. To unassign a sign out reason from the team, click 'x' next to the reason in **List of Sign Out Reasons**.
Wrap-Up Reasons	To assign wrap-up reasons to the team: **a.** Click the + icon. The **Add Wrap-Up Reasons** pop-up window opens with a list of wrap-up reasons. The reasons are configured as **Team Specific** in **Desktop** > **Reason Labels**. **b.** Select one or more reasons from the list. Use the Sort a List and Search a List features to navigate the list. The selected reasons are highlighted in the popup window, and appear in **List of Wrap-Up Reasons**. You can click the **Label** header to sort the reasons. To unassign a wrap-up reason from the team, click 'x' next to the reason in **List of Wrap-Up Reasons**.

Workflows	To assign workflows to the team: **a.** Click the + icon. The **Add Workflow** pop-up window opens with a list of workflows that are configured for the site in **Desktop** > **Resources** > **Workflows**. **b.** Select one or more workflows from the list. Use the Sort a List and Search a List features to navigate the list. **Note** You cannot search the list by description in the pop-up window. The selected workflows are highlighted in the pop-up window, and also appear in **List of Workflows**. **c.** Close the **Add Workflow** pop-up window. The workflows are carried out in the order they appear in the **List of Workflows**. The **Order** column displays the order of the workflow. The newly added workflow appears at the end of the list. **d.** To change the workflow order: **1.** In the **Order** column, click the drop-down arrow that is associated with the workflow that you want to move. The values in the drop-down are the number of workflows that are selected for the team. The number increments or decrements dynamically when you assign or unassign the workflow. **2.** Select a number from the drop-down list. The workflow moves to the selected position in the **List of Workflows** table. The other workflows move a row up or down based on the new position of the workflow. To unassign a workflow from the team, click 'x' next to the workflow in **List of Workflows**.

Step 7 Click **Save** to return to the List window, where a message confirms the successful creation of the team. The team and the associated agents or supervisors appear in the List window. When you create a team in Packaged CCE, the same team record is also created as a collection in Cisco Unified Intelligence Center. The team resources that are assigned to the team appear in Cisco Finesse Admin.

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

Example:

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

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?
        gadgetHeight=310&viewId_1=99E6C8E2100001410000000D80A0006C4&
        filterId_1=agent.id=CL%20teamName&viewId_2=9AB7848B10000141000001C50A0006C4&
        filterId_2=agent.id=CL%20teamName
        </gadget>
```

Step 2 Go to **Organization** > **Teams**, and open an existing team's record on the list window.

Step 3 Click the **Team Resources** tab.

Step 4 In the **Desktop Layout** tab, check the **Customize** check box.

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=99E6C8E2100001410000000D80A0006C4&
              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=99E6C8E2100001410000000D80A0006C4&
        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.

Note You can also perform the above steps in Unified CCE Administration (https://<Side A/B Unified CCE AW-HDS-DDS IP address>/cceadminnew). In Unified CCE Administration, you can navigate to Desktop > Resources to copy the XML code from default layout, and then navigate to Organization > Teams to access the Team Resources paste the XML.

Search for Teams

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

Click the + icon at the right of the Search field in the Team tool. In the popup window, you can:

- Search for a name or description.
- 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 peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

  If you select **Globals and Departments** or **Departments only**, you can only enter a space-separated list of department names. (Department is an OR search.)

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

Search by site is available only when remote sites are configured.

Manage Skills

Calls are queued to agents based on their membership in skill groups or their qualification in precision queues.

Administrators have access to all tools documented in this chapter .

Supervisors have limited access to Skill Groups and display-only access to Attributes and Precision Queues.

Skill Groups

A skill group is a collection of agents who share a common set of competencies that equip them to handle the same types of requests. Some examples of skill groups are a collection of agents who speak a specific language or who can assist callers with billing questions.

An agent can be a member of multiple skill groups. Each skill group is associated with a specific media routing domain (MRD) such as voice, chat, or email.

An agent's skill group membership can determine the types of contacts that are routed to that agent. For example, if an agent is a member of a skill group that is set up for the Cisco_Voice routing domain only, then that agent is a voice agent for that skill group. If an agent is a member of a skill group that is set up for a nonvoice routing domain, then that agent is a multichannel agent for that skill group.

Use Cisco Unified Intelligence Center reports to view agent activity in skill groups, to monitor call distribution among skill groups, or to see how one skill group is performing compared with others.

Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Skill Groups** to configure skill groups.

Administrators have full permission to configure skill groups. Supervisors have permission to add and remove their supervised agents on the Skill Groups Members tab.

Related Topics

Search for Skill Groups, on page 109
Add and Maintain Skill Groups, on page 106
Agents, on page 79
Skill Groups or Precision Queues?, on page 112
Manage Supervisors, on page 89

Add and Maintain Skill Groups

Procedure

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

Step 2 Click **New** to open the **New Skill Group** window.

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

Field	Required	Description
Name	yes	Enter a name using up to 32 alphanumeric characters.
Description	no	Enter up to 255 characters to describe the skill group. See Character Sets.

Field	Required	Description
Site	-	The **Site** field displays Main by default for Packaged CCE 2000 Agents deployment type. To add a different site: **a.** Click the **magnifying glass** icon to display the list of sites with Agent PG configured. **b.** Select the required site.
Peripheral Set	yes	**Note** Before you add a **Peripheral Set**, you must select a **Site**. The **Peripheral Set** field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set. To select a peripheral set: **a.** Click the **magnifying glass** icon to display the list of peripheral sets configured for the selected **Site**. **b.** Select the applicable peripheral set.
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*. To select a different Media Routing Domain: **a.** Click the **magnifying glass** icon to display **Select Media Routing Domain** . **b.** Click a row to make a selection and close the list.

Field	Required	Description
Bucket Interval	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, see Global, on page 210. To select a different bucket interval: **a.** Click the **magnifying glass** icon to display **Select Bucket Intervals**. **b.** Click a row to make a selection and close the list. Click the **x** icon to clear the selection.
Service Level Threshold	no	Enter a value in seconds that you set as a goal for connecting a call with an agent. The field defaults to the threshold configured for this Media Routing Domain. Leave this field blank to use the service level threshold value for the Media Routing Domain. Enter a value of 0 seconds if you do not want a service level event to be set for the calls. These calls are not treated as service-level calls.
Service Level Type	no	Select a service level type. Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation. • **Use Media Routing Domain Value** (the default): Select this option to use the value that is currently defined for the MRD. • **Ignore Abandoned Calls:** Select this option if you want abandoned calls to be excluded from the service level calculation. • **Abandoned Calls have Negative Impact:** Select this if you want only calls that are answered within the service level threshold time as to be counted as treated calls. The service level is negatively affected by calls that abandon within the service level time. • **Abandoned Calls have Positive Impact:** Select this if you consider a call abandoned within the service level threshold time as a treated call. With this configuration, abandoned calls have a positive impact on the service level.

Step 4 Complete the **Members** tab:

This tab shows the list of agents for this skill group.

a) Click the + icon to open **Add Agents**. The agents associated to the selected site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) display.
b) Click the agents you want to add to this skill group.
c) Close the window. The agents you chose appear on the **List of Agents**.
d) Click **Save** on this tab to return to the List window, where a message confirms the successful creation of the skill group.

Search for Skill Groups

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

Click the + icon in the Search field to open a popup window, where you can:

- Enter a 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 peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

  Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Department is an OR search.)

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

Search by site is available only when remote sites are configured.

Attributes

Attributes identify a call routing requirement, such as language, location, or agent expertise. You can create two types of attributes: Boolean or Proficiency.

- Use Boolean attributes to identify an agent attribute value as true or false. For example, you can create a Boston attribute that specifies that the agent assigned to this attribute must be located in Boston. An agent in Boston would have *Boston = True* as the term for that attribute.
- Use Proficiency attributes to establish a level of expertise in a range from 1 to 10, with 10 being the highest level of expertise. For a Spanish language attribute, for example, an original speaker would have the attribute *Proficiency = 10*.

When you create a precision queue, you identify which attributes are part of that queue and then implement the queue in a script. When you assign a new attribute to an agent and the attribute value matches the precision queue criteria, the agent is automatically associated with the precision queue.

An attribute can be associated with more than one precision queue, from multiple Media Routing Domains.

Navigate to **Unified CCE Administration** > **Organization** > **Skills** and click the **Attributes** tab to configure attributes.

Administrators can see and manage attributes. Supervisors can configure attributes for their supervised agents on the Attributes tab of the Agents tool.

Related Topics

Add and Maintain Attributes, on page 110
Precision Queues, on page 111

Add and Maintain Attributes

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Organization** > **Skills** and click the **Attributes** tab.

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. See Character Sets.
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 To associate one or more agents to this attribute, click on the **Agents** tab, and then click **New**.

Step 5 Click **Add**.

Step 6 In the **Add Agents** window, click on one or more of the agents listed to add them to the **List of Agents** window. Once you are finished, close the window.

Step 7 Set the attribute value as appropriate for each agent using the **Attribute Value** drop-down menus.

Step 8 Click **Save**.

Precision Queues

Precision routing offers a multidimensional 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 caller's precise needs. Precision queues are the key components of precision routing.

To configure Precision Routing, you must do the following:

1. Create attributes. Attributes are characteristics that can be assigned a True | False value or a Proficiency rating from 1 to 10.
2. Assign attributes to agents.
3. Create precision queues.
4. Create routing scripts.

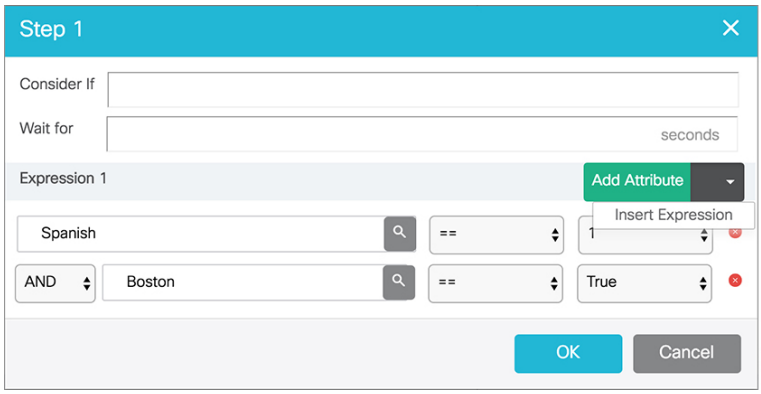
There is no need to add an agent to a precision queue; agents become members of precision queues automatically based on their attributes. If a precision queue requires an agent who lives in Boston, who speaks fluent Spanish, and who is proficient in troubleshooting a specific piece of equipment, an agent with the attributes *Boston = True*, *Spanish = True*, and *Repair = 10* is automatically part of the precision queue. A Spanish caller in Boston who needs help with equipment is routed to that agent.

A precision queue includes:

- **Terms:** A term compares an attribute against a value. For example, you can create the following term: Spanish == 10. The term of the attribute is the highest proficiency in Spanish.

  Each precision queue can have multiple attributes, and these attributes can be used in multiple terms. For example, to select an agent with a Spanish proficiency value between 5 and 10, you would create one term for Spanish > 5 and another for Spanish < 10.

- **Expressions:** An expression is a collection of one or more terms. The terms in an expression must share the same operator—they must all be AND or must all be OR relationships.



- **Steps:** A precision queue step is a time-based routing point within the precision queue. A step is a collection of one or more expressions.

  A step may also include wait time and a Consider If formula. Use wait time to assign a maximum amount of time to wait for an available agent. Use a Consider If formula to evaluate the step against predefined criteria, for example, another queue.

Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Precision Queues** to configure precision queues.

Navigate to **Unified CCE Administration** > **Organization** > **Skills** > **Precision Queues** to configure precision queues.

Administrators have full permission to configure precision queues. Supervisors have display-only access to the Precision Queues tool.

When you add or modify precision queues associated with a large number of agents, the system avoids potential overload conditions by updating the agent associations as system resources allow. Precision queue updates may be rejected if the system is too busy.

Skill Groups or Precision Queues?

Should you use skill groups or precision queues for the routing needs of your organization? This section distinguishes the two methods.

Use a Skill Group

A skill group represents a competency or responsibility. For example, it could be a predefined collection of traits, such as salespeople who are in charge of selling to England. The skill group could be called “English sales”. If you wanted to divide the agents in this group into two types of proficiencies (perhaps based on experience), you would need to set up two separate skill groups; for example, English Sales 1 and English Sales 2. You would then associate an agent with one of them, based on the agent's proficiency. Do this by accessing the skill group and locating the agent that you want to add to it (or add that skill group to the agent). To summarize, creating a skill group involves first building a concept of what combinations of traits you want for each agent, like English Sales 2.

Use a Precision Queue

In contrast to skill groups, a precision queue breaks down attribute definitions to form a collection of agents at an *attribute* level. The agents that match the attribute level of the precision queue become associated with that precision queue.

With precision queues, the preceding English sales example involves defining the attributes English and Sales, and associating agents that have those traits to them. The precision queue English Sales would dynamically map all those agents that had those traits to the precision queue. In addition, you can define more complex proficiency attributes to associate with those agents. This would allow you to build, in a single precision queue, multiple proficiency searches like English language proficiency 10 and sales proficiency 5.

To break down the precision queue example into skill groups, you would need to set up two separate skill groups: English language proficiency 10 and sales proficiency 5. With precision queues, you can refine agents by attributes. With skill groups, you define a skill group and then assign agents to it.

Decide on Skill Groups or a Precision Queue

Precision routing enhances and can replace traditional routing. Traditional routing looks at all of the skill groups to which an agent belongs and defines the hierarchy of skills to map business needs. However, traditional routing is restricted by its single-dimensional nature.

Precision routing provides multidimensional routing with simple configuration, scripting, and reporting. Agents are represented through multiple attributes with proficiencies so that the capabilities of each agent are accurately exposed, bringing more value to the business.

If your routing needs are not too complex, consider using one or two skill groups. However, if you want to conduct a search involving as many as ten different proficiency levels in one easily managed queue, use precision queues.

Add and Maintain Precision Queues

Before you begin

Before you can create precision queues, you must create attributes (see Add and Maintain Attributes, on page 110).

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
Name	yes	Enter up to 32 alphanumeric characters.
Description	no	Enter up to 255 characters to describe the precision queue. See Character Sets.
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*. To select a different Media Routing Domain: **a.** Click the **magnifying glass** icon to display **Select Media Routing Domain** . **b.** Click a row to make a selection and close the list.

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 (see Global, on page 210). To select a different bucket interval: **a.** Click the **magnifying glass** icon to display **Select Bucket Intervals**. **b.** Click a row to make a selection and close the list.

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**.

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.

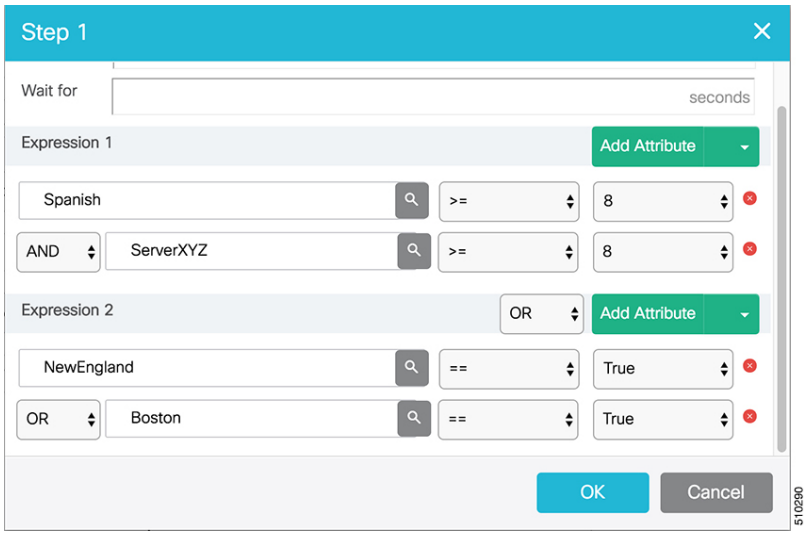
All attributes within an expression must be joined by the same logical operator. They must all be ANDs, or they must all be ORs.

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 117 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.

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.

Precision Queue Call Flow Example

At a high level, consider a 5-step precision queue with a Consider If formula for *Caller is Premium Member* attached to the Step 1:

- Step 1 - Attribute: Skill > 8 - Consider If: Caller is Premium Member
- Step 2 - Attribute: Skill > 6
- Step 3 - Attribute: Skill > 4
- Step 4 - Attribute: Skill > 3
- Step 5 - Attribute: Skill >= 1

Caller John, who is not a premium customer, calls 1-800-repairs. John's call is routed to this precision queue.

- Since John is not a premium customer, John is immediately routed out of Step 1 (because of the Consider If on Step 1) and into Step 2 where John waits for the call to be answered.
- After the Step 2 wait time has expired, John's call moves to Step 3 to wait for an agent.
- After the Step 3 wait time has expired, John's call moves to Step 4 to wait for an agent.

- When it arrives at Step 5, John's call will wait indefinitely for an available agent. This step cannot be avoided by any call because there is no routing logic past this.

The overarching idea is that customer will use each successive step to expand the pool of available agents. Eventually, when you reach the "last" step (the step with the highest number), the call is waiting in a potentially very large pool of agents. With each extra step, the chances of the call being handled increase. This also puts the most valuable and skilled agents in the earlier precision queue steps. Calls come to them first before moving on the less appropriate agents in later steps.

Note When two or more agents have the same proficiently level for the attributes the PQ step leverages the Longest Available Agent (LLA).

Manage Departments

Departments

You have the option to create departments to facilitate contact center operation and maintenance. A contact center for a hospital might create departments for Surgery, Radiology, Obstetrics, and other operational units. A contact center for a university might create departments for Admissions, Alumni, and Registration. Departments are not required, and there are no built-in departments.

If you do not create departments, all administrators and objects are *global*, meaning that they are not associated with a department.

If you create departments, you have the option to associate a department with each administrator and object. These are called *departmental* administrators and objects. Your Packaged CCE configuration can include a mix of global and departmental administrators and objects.

You can creating routing scripts for a department by referencing objects from that department in the scripts.

You can also create custom reporting collections in Cisco Unified Intelligence Center to report on departmental objects. See the *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 for directions on customizing reports.

Departmental Objects

The following objects can be associated with a single department. If departments are configured, the List screens for these objects have a Department column. The New and Edit windows for these objects have a Department field.

- Agents
- Attributes
- Bucket intervals
- Call types
- Desk settings
- Dialed numbers

- Network VRU scripts
- Precision queues
- Skill groups
- Teams

Relationships Between Global and Departmental Objects

You can create relationships between objects in your configuration. For example, you can associate an agent with skill groups, a call type with a dialed number, and so on. An object's department assignment controls the relationships it can have to other objects.

The rules for creating relationships between objects are as follows:

- A **global** object can be associated with any global or departmental objects. For example, when you are assigning skill groups to a global agent, the skill group selection list includes global skill groups and skill groups in all departments to which you have access.
- A **departmental** object can be associated with global objects or with objects in the same department. For example, when you are assigning skill groups to an agent in Department A, the skill group selection list includes global skill groups and skill groups in Department A.

These rules are summarized in the following table.

Table 18: Rules for Relationships Between Global and Departmental Objects

Object Type	Can be associated with Global object?	Can be associated with Departmental object?
Global	yes	yes, with objects from any department
Departmental	yes	yes, with objects from same department only

The only exceptions to these rules are for the relationships between the following objects:

- **Teams and agent:** A global agent can belong only to a global team. A departmental agent can belong either to a global team or to a team that is associated with the same department.
- **Teams and supervisors:** Global supervisors can supervise both global and departmental teams. Departmental supervisors can supervise only teams that are associated with the same department.

These exceptions prevent departmental supervisors from modifying global agents, and are summarized in the following table.

Table 19: Rules for Relationships Between Teams and Agents and Teams and Supervisors

	Agent - Global	Agent - Departmental	Supervisor - Global	Supervisor - Departmental
Team - Global	yes	yes	yes	no
Team - Departmental	no	yes (same department only)	yes	yes (same department only)

Change Departments for an Object

When you change the department for an object, relationships with objects in the original department are cleared; relationships with global objects and objects in the new department remain intact. For example, if you change an agent from Department A to Department B, any skill groups in Department A that had been associated with the agent are cleared.

For some objects, such as call type, the Edit window does not show all related objects. If you try to change the department for those objects, you see an error indicating that you cannot change the department because a related object is in the original department. For example, you see this error if you try to change a call type from Department A to Department B and it is related to a dialed number in Department A. You must change the department of the dialed number before you can change the department of the call type.

System-wide Settings and Global Objects

Only global objects can be selected for system-wide settings in the **Call Settings** > **Labels**.

Global and Departmental Administrators

When you create administrators, you can configure them as global administrators or associate them with departments. See Add and Maintain Administrators, on page 94.

Global administrators

Global administrators:

- Have read and write access to departmental objects and global objects on all tools and menus that are allowed for their role.
- Can use Script Editor or Internet Script Editor to modify routing scripts.

Departmental administrators

Departmental administrators:

- Can be associated with multiple departments. They have read and write access to global objects and objects in their departments on all tools and menus that are allowed for their role.
- A departmental administrator with the ConfigAdmin role has read-only access to the General tools on the System menu: Information, Settings, Deployment, and Agent Trace.
- Can use Internet Script Editor to modify scripts that reference objects associated with their departments. Departmental administrators cannot log into Script Editor.

Add and Maintain Departments

To add, edit, or delete departments, an administrator must have the SystemAdmin role.

This procedure explains how to add a department. For information on maintaining departments, see Update Objects, on page 4 and Delete Objects, on page 7.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Organization** > **Departments**.

A **List of Departments** window opens.

Step 2 Click **New** to open the **New Department** window.

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

a) **Name** (Required) Enter a unique name for the department, using a maximum of 32 characters.

b) **Description** (Optional) Enter a maximum of 255 characters to describe the department. See Character Sets for details on valid characters for this field.

Step 4 Click the **Administrators** tab.

This tab shows the Username and Domain of the administrators who currently serve as department administrators and allows you to add or remove administrators.

a) Click the + icon to open the **Add Administrators** popup window.

b) Click one or more rows to select administrators; then close the popup window. The administrators are now on the List of Administrators.

c) Click the **x** icon to remove an administrator from the list.

Step 5 Click **Save** to return to the list window, where a message confirms the successful creation of the department.

Manage Campaigns

Add and Maintain Agent Based Campaigns

This procedure explains how to add an agent based campaign. For information on maintaining campaigns, see Update Objects and Delete Objects.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Campaigns**.

Step 2 On the **Campaigns** page, click **New** and then choose **Agent Based**.

Step 3 On the **New Agent Based Campaign**, complete the following information on the **General** tab.

Field	Required?	Description
Name	Yes	Enter a unique name for the campaign. Maximum length is 32 characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric. **Note** You cannot use the system reserved terms such as **dnc** and **none** as a campaign name.
Status	-	The option to enable or disable the campaign. It is enabled by default.
Type	-	Displays **Agent Based** by default.

Field	Required?	Description
Dialing Mode	Yes	Select a dialing mode from the drop-down list. • **Predictive**: The Dialer component determines the number of customers to dial per agent, based on the abandoned rate. The agent must take the call if logged in to a campaign skill group. • **Progressive**: The administrator specifies a fixed number of lines to dial per agent instead of the Dialer component determining the number of lines. The agent must take the call if logged in to a campaign skill group. • **Preview**: The agent previews customer information on their desktop, and chooses to contact the customer, skip to another customer, or reject the call. • **Preview Direct**: This is similar to the Preview mode, except that the dialer automatically dials the call from the agent's phone after the agent accepts.
Description	No	Enter up to 255 characters to describe the campaign. See Character Sets.
Schedule section		
Start Date	No	The date that the campaign starts.
End Date	No	The date that the campaign ends.
Start Time	Yes	The time the campaign starts dialing customer numbers.
End Time	Yes	The time the campaign stops dialing customer numbers.
Time Zone	Yes	The time zone where the campaign runs.
Dialing Option section **Note** This section appears only after you select the **Dialing Mode** as **Predictive** or **Progressive**.		
Lines Per Agent	No	The number of lines dedicated to each agent in the campaign. Range is 1 – 100. Default is 1.5.
Maximum Lines Per Agent	No	This field appears only after you select the **Dialing Mode** as **Predictive**. The upper bound for the number of customers the dialer dials for a reserved agent when a campaign is running in predictive mode. Range is 1 – 100. Default is 2.

Field	Required?	Description
Call Abandon Limit	-	This field appears only after you select the **Dialing Mode** as **Predictive**. A call is considered abandoned if a person answers it and the contact center does not connect the call to an agent within two seconds of the person's completed greeting. The granularity is to one-tenth of a percent. Default is 3.
Limit	No	You can set the limit for abandon calls only after you enable the **Call Abandon Limit** option. You can set a limit (0.1-100) for the percentage of abandoned calls in a campaign. If the **Call Abandon Limit** option is disabled, the campaign dials without regard to the abandon limit.
Call Progress Analysis (CPA)	-	Enabled by default. **Note** If you keep it enabled, make sure you have configured and enabled Call Progress Analysis in the Voice Gateway.
Record CPA	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files.
Answering Machine Treatment	-	Enabled by default. This enables the dialer to detect an answering machine. From the drop-down list, choose one of the following actions that the dialer must perform when the dialer detects an answering machine: • **Abandon Call**: Drops the call, marks it as an answering machine, and schedules a retry. This option is selected by default. • **Transfer to Agent**: Transfers the call to an agent. • **Transfer to IVR Route Point**: Transfers the call to play a prerecorded message. The IVR route point is configured in the **Skill Group selection** dialog box on the **Skill Groups** tab.
Terminate Tone Detect	-	This field is activated only when the **Answering Machine Treatment** field enabled and you select the **Transfer to IVR Route Point** option from the drop-down list. You can enable this field to allow the dialer to transfer the call to IVR route point after detecting the answering machine beep.
Callback Settings section		
Personalized Callback	-	Enable this option allows an agent to schedule a callback to a customer for a specific date and time. A personal callback connects the same agent who initiated the callback to the customer.

Field	Required?	Description
Missed Callback	Yes (When **Personalized Callback** option is enabled.)	Select an option from the drop-down list to handle the personal callback in case the agent is not available. • **Abandon**: Abandon the personal callback. This option is selected by default. • **Same time next business day**: Reschedule the personal callback to the same time the next business day. • **Use campaign dialed number**: Use the alternate dialed number.

Step 4 On the **Skill Group** tab, click **Add** to open the **Add Skill Group** pop-up window.

Note You must add at least one Skill Group for a campaign.

Step 5 Complete the following information in the **Add Skill Group** pop-up window.

Field	Required?	Description
Site	Yes	Select a site from the drop-down list. Based on the site, you can select peripheral set, skill group and dialed number in the subsequent fields.
Peripheral Set	Yes	This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set. Select a peripheral set from the drop-down list. The list contains the peripheral sets associated to the selected site.
Skill Group	Yes	Click the **Search** icon to open the **Add a Skill Group** pop-up. You can search and select the Skill Group based on the name and description. The search result does not display the Skill Groups that are already added to a Campaign.
Dialed Number	Yes	Click the **Search** icon to open the **Add Dialed Number** pop-up. By default, you can view all the dialed numbers for which the **Routing Type** is set as **Outbound Voice**. You can search and select the dialed number based on the string value and description. The search result does not display the dialed numbers that are already added to a Campaign. The selected number is dialed to reserve an agent in the configured skill group.

Field	Required?	Description
Contact Records Cache Size	No	Enter the minimum number of dialing numbers that each dialer caches for each of the Outbound Option skill groups. Range is 1 – 400. Default is 1.
Reserve Additional Agents	No	This field is available only if the dialing mode is selected as **Preview** or **Preview Direct** on the **General** tab. Enter the number of agents reserved for the campaign. This ensures that there is always at least one extra agent reserved before the dialer begins dialing. Range is 0 – 100. Default is 0.
Dialed Numbers for Transferring to an IVR Section		
Answering machine to IVR	No	Click the **Search** icon to open the **Add Dialed Number** pop-up. By default, you can view all the dialed numbers for which the **Routing Type** is set as **Outbound Voice**. You can search and select the dialed number based on the string value and description. The selected number indicates the route point required to do the transfer to IVR routing script.
Agent not available for IVR	No	Click the **Search** icon to open the **Add Dialed Number** pop-up. By default, you can view all the dialed numbers for which the **Routing Type** is set as **Outbound Voice**. You can search and select the dialed number based on the string value and description. The selected number is dialed to play a message to the calls about to be disconnected due to lack of available agents.

Step 6 Click **Add**.

Note To delete the Skill Groups from the campaign, check the check box corresponding to Skill Groups on the **Skill Group** tab and click **Delete** and confirm your intention to delete.

Or

Hover the mouse pointer over the row for a Skill Group to see the **delete (x)** icon at the end of the row. Click the **x** icon and confirm your intention to delete.

Step 7 Click the **Advanced** tab and complete the following information:

Field	Required?	Description
Dialing Option section		
No answering ring limit	No	Enter the number of times the system allows a dialed phone number to ring. Range is 2 – 10. Default is 4.
Maximum attempts	No	Enter the maximum number of attempts, including callbacks and retries. Range is 1 – 100. Default is 3.

Field	Required?	Description
Abandoned call wait time	Yes	Enter the minimum duration (in seconds) of an outbound call. Range is 0 – 10. Default is 1. **Note** If the call duration is less than the specified value, the system considers the call to be customer abandoned and schedules the record for a retry. To disable this feature, set the parameter to 0.
Campaign prefix digits	No	Enter the digits to prefix to each customer number dialed from this campaign. Maximum length is 15 digits.
Retries section		
No answer delay	No	Enter the time (in minutes) the dialer waits before calling back a no-answer call. Range is 1 – 99999. Default is 60.
Busy signal delay	No	Enter the time (in minutes) the dialer waits before calling back a busy phone number. Range is 1 – 99999. Default is 60.
Customer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if a customer abandons a call. Range is 1 – 99999. Default is 30.
Dialer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if the dialer abandons a call. Range is 1 – 99999. Default is 60.
Answering machine delay	No	Enter the time (in minutes) the dialer waits before calling back, if an answering machine answers a call. Range is 1 – 99999. Default is 60.
Customer not home delay	No	Enter the time (in minutes) the dialer waits before calling back, if a customer is not home. Range is 1 – 99999. Default is 60.
Call Progress Analysis(CPA) Parameters section		
Minimum Silence Period(100-1000)	No	Minimum silence period required to classify a call as voice detected. If many answering machine calls are being passed through to agents as voice, then increasing this value accounts for longer pauses in answering machine greetings. Default is 608.
Analysis Period(1000-10000)	NO	Number of milliseconds spent analyzing this call. If there is a short agent greeting on an answering machine, then a longer value here categorizes that answering machine call as voice. If the call is to a business where the operator has a longer scripted greeting, a shorter value here categorizes the long, live greeting as answering machine. Default is 2500.
Minimum Valid Speech(50-500)	NO	Minimum number of milliseconds of voice required to qualify a call as voice detected. Default is 112.
Maximum Analysis Time(1000-10000)	NO	Maximum number of milliseconds allowed for analysis before identifying a problem analysis as dead air/low volume. Default is 3000.

Field	Required?	Description
Maximum termination tone analysis(1000-60000)	NO	Maximum milliseconds the dialer analyzes an answering machine voice message looking for a termination tone. If the message has an odd tone and the analysis does not recognize it, the call is not transferred or dropped until this timeout occurs. Default is 30000.

Step 8 Click **Save**.

Add and Maintain IVR Based Campaigns

This procedure explains how to add an IVR Based outbound campaign map the Skill Groups for the campaign. For more information about maintaining campaigns, see Update Objects and Delete Objects.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Campaigns** to open the **Campaigns** page.

Step 2 Click **New** and choose **IVR Based** to open the **New IVR Based Campaign** page.

Step 3 Complete the following information on the **General** tab.

Field	Required?	Description
Name	Yes	Enter a unique name for the campaign. Maximum 32-character string, including alphanumeric characters, periods (.), and underscores (_). Alphabetic characters can be upper or lowercase. The name must begin with an alphanumeric character. **Note** You cannot use the system reserved terms such as **dnc** and **none** as a campaign name.
Status	-	The option to enable or disable the campaign. It is enabled by default.
Type	-	The default field value is set to **IVR Based**. You cannot edit this field.
Dialing Mode	Yes	From the drop-down list, choose the dialer type for the current IVR campaign. • **Predictive**: The dialer component determines the number of customers to dial per IVR port, based on the abandoned rate. • **Progressive**: The administrator specifies a fixed number of lines to dial per IVR port. **Note** An unattended campaign can use either the Progressive or Predictive mode. You can play a different prompt for a live customer or for an answering machine.
Description	No	Enter a description about the campaign using up to 255 characters. See Character Sets.

Field	Required?	Description
Schedule section		
Start Date	No	Select the date that the campaign starts.
End Date	No	Select the date that the campaign ends.
Start Time	Yes	Enter the time that the campaign starts dialing the customer numbers.
End Time	Yes	Enter the time that the campaign stops dialing the customer numbers.
Time Zone	Yes	Choose the time zone where the campaign runs.
Dialing Option section		
Lines Per Agent	No	The number of lines dedicated to each IVR port for the campaign. Range is 1 – 100. Default is 1.5.
Maximum Lines Per Agent	No	This field appears only after you select the **Dialing Mode** as **Predictive**. The upper bound for the number of customers the dialer dials for a reserved IVR port when a campaign is running in predictive mode. Range is 1 – 100. Default is 2.
Abandon Calls Limit	-	This field appears only after you select the **Dialing Mode** as **Predictive**. A call is considered abandoned if a person answers it and the contact center does not connect the call to IVR within two seconds of the person's completed greeting. The granularity is to one-tenth of a percent. Default is 3.
Limit	No	You can set the limit for abandon calls only after you enable the **Call Abandon Limit** option. You can set a limit (0.1-100) for the percentage of abandoned calls in a campaign. If the **Call Abandon Limit** option is disabled, the campaign dials without regard to the abandon limit.
Call Progress Analysis (CPA)	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files. **Note** If you keep it enabled, make sure you have configured and enabled Call Progress Analysis in the Voice Gateway.
Record CPA	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files.

Field	Required?	Description
Answering Machine Treatment	-	This field is enabled by default to allow the dialer to detect an answering machine. From the drop-down list, choose one of the following actions that the dialer must perform when the dialer detects an answering machine: • **Abandon Call**: Drops the call, marks it as an answering machine, and schedules a retry. This option is selected by default. • **Transfer to IVR Route Point**: Transfers the call to play a prerecorded message. The IVR route point is configured in the **Skill Group selection** dialog box on the **Campaign Skill Groups** tab. **Note** After you configure a Transfer to IVR Route Point, you cannot set the AMD records as **Retry**. Use a customized query to identify such calls and create a new campaign.
Terminate Tone Detect	-	This field is activated only when the **Answering Machine Treatment** field enabled and you select the **Transfer to IVR Route Point** option from the drop-down list. You can enable this field to allow the dialer to transfer the call to IVR route point after detecting the answering machine beep.
Callback Settings section		
Personalized Callback	-	Enable this option allows the IVR port to schedule a callback to a customer for a specific date and time.
Missed Callback	Yes (When **Personalized Callback** option is enabled.)	Select an option from the drop-down list to handle the personal callback in case the agent is not available. • **Abandon**: Abandon the callback. This option is selected by default. • **Same time next business day**: Reschedule the callback to the same time the next business day. • **Use campaign dialed number**: Use the alternate dialed number.

Step 4 Click the **Skill Group** tab and then click the **Add** button to add the skill groups for the current IVR campaign.

Note You must add at least one Skill Group for a campaign.

Step 5 Complete the following information in the **Add Skill Group** pop-up window.

Field	Required?	Description
Site	Yes	Select a site from the drop-down list. Based on the site, you can select peripheral set, skill group and dialed number in the subsequent fields.

Field	Required?	Description
Peripheral Set	Yes	This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set. Select a peripheral set from the drop-down list. The list contains the peripheral sets associated to the selected site.
Skill Group	Yes	Click the **Search** icon to open the **Add a Skill Group** pop-up. You can search and select the Skill Group based on the name and description. The search result do not display the Skill Groups that are already added to a Campaign.
Dialed Number	Yes	Click the **Search** icon to open the **Add Dialed Number** pop-up. By default, you can view all the dialed numbers for which the **Routing Type** is set as **Outbound Voice**. You can search and select the dialed number based on the string value and description. The search result do not display the dialed numbers that are already added to a Campaign. The selected number is dialed to reserve an IVR port in the configured skill group.
Contact Records cache Size	Yes	Enter the minimum number of dialing numbers that each dialer caches for each of the Outbound Option skill groups. Range is 1 – 400. Default is 1.
Number of IVR Ports	No	Enter the total number of IVR ports allocated for the specified skill group. This value indicates how many ports are available for the dialer to transfer customer calls. The application uses one IVR to play different messages based on the route point where the contact is transferred. If there are multiple dialers associated with this skill group, each dialer dials a fraction of the total number of ports.
Dialed Numbers for Transferring to an IVR Section		
Answering Machine to IVR	Yes	Click the **Search** icon to open the **Add Dialed Number** pop-up. By default, you can view all the dialed numbers for which the **Routing Type** is set as **Outbound Voice**. You can search and select the dialed number based on the string value and description. When the dialer identifies the answering machine, the selected number is dialed to transfer the call to IVR routing script. The routing script transfers the call to an IVR.

Step 6 Click **Add**.
The newly added Skill Group is displayed on the **Skill Group** tab for the current campaign.

Note To delete the Skill Groups from the campaign, check the check box corresponding to Skill Groups on the **Skill Group** tab and click **Delete**, and confirm your intention to delete.

Or

Hover the mouse pointer over the row for a Skill Group to see the **delete (x)** icon at the end of the row. Click the **x** icon and confirm your intention to delete.

Step 7 Click the **Advanced** tab and complete the following information.

Field	Required?	Description
Dialing Option section		
No answering ring limit	No	Enter the number of times the system allows a dialed phone number to ring. Range is 2 – 10. Default is 4.
Maximum attempts	No	Enter the maximum number of attempts, including callbacks and retries. Range is 1 – 100. Default is 3.
Abandoned call wait time	Yes	Enter the minimum duration (in seconds) of an outbound call. Range is 0 – 10. Default is 1. **Note** If the call duration is less than the specified value, the system considers the call to be customer abandoned and schedules the record for a retry. To disable this feature, set the parameter to 0.
Campaign prefix digits	No	Enter the digits to prefix to each customer number dialed from this campaign. Maximum length is 15 digits.
Retries section		
No answer delay	No	Enter the time (in minutes) the dialer waits before calling back a no-answer call. Range is 1 – 99999. Default is 60.
Busy signal delay	No	Enter the time (in minutes) the dialer waits before calling back a busy phone number. Range is 1 – 99999. Default is 60.
Customer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if a customer abandons a call. Range is 1 – 99999. Default is 30.
Dialer abandoned delay	No	Enter the time (in minutes) the dialer waits before calling back, if the dialer abandons a call. Range is 1 – 99999. Default is 60.
Call Progress Analysis(CPA) Parameters section		
Minimum Silence Period(100-1000)	No	Minimum silence period required to classify a call as voice detected. If many answering machine calls are being passed through to agents as voice, then increasing this value accounts for longer pauses in answering machine greetings. Default is 608.

Field	Required?	Description
Analysis Period(1000-10000)	NO	Number of milliseconds spent analyzing this call. If there is a short agent greeting on an answering machine, then a longer value here categorizes that answering machine call as voice. If the call is to a business where the operator has a longer scripted greeting, a shorter value here categorizes the long, live greeting as answering machine. Default is 2500.
Minimum Valid Speech(50-500)	NO	Minimum number of milliseconds of voice required to qualify a call as voice detected. Default is 112.
Maximum Analysis Time(1000-10000)	NO	Maximum number of milliseconds allowed for analysis before identifying a problem analysis as dead air/low volume. Default is 3000.
Maximum termination tone analysis(1000-60000)	NO	Maximum milliseconds the dialer analyzes an answering machine voice message looking for a termination tone. If the message has an odd tone and the analysis does not recognize it, the call is not transferred or dropped until this timeout occurs. Default is 30000.

Step 8 Click **Save**.

Edit Contacts

This procedure explains how to upload contacts to newly created campaigns. You can also use this procedure to edit the contacts of existing campaigns.

Procedure

Step 1 On the **Campaigns** page, select one or more campaigns.

Step 2 Choose **Edit** > **Contacts** to open the **Edit Campaign** page.

Step 3 Click the download icon next to **Download Contacts Template (csv)** to download the contacts template. You can use this template to enter contacts and upload.

Step 4 Click the download icon next to **Download All Contacts (csv)** to download all existing contacts in the campaign.

Step 5 Click **Choose File** and upload the contacts file.

Note The file must be in CSV format with a file extension as .txt or .csv.

The file must contain at least one phone number without any special characters.

Step 6 Check the **Delete Existing Contacts** check box to delete the existing contacts in the selected campaigns.

Note While uploading the contacts file, if you do not check the **Delete Existing Contacts** check box, the uploaded contacts are appended to the existing contacts.

Step 7 Click **Save** and then click **Yes** to confirm the changes.

Edit Status and Schedule

This procedure explains how to edit the status and schedule of campaigns.

Procedure

Step 1 On the **Campaigns** page, select one or more campaigns to edit.

Step 2 Choose **Edit** > **Status and Schedule** to open the **Edit Campaign** page.

- If you have selected one campaign, edit the status and the schedule of the campaign.
- If you have selected multiple campaigns,
  a. Check the **Edit Status** check box and edit the status of the campaign.
  b. Check the **Edit Schedule** check box to enable the fields under **Schedule** and select new values.

Step 3 Click **Save** and then click **Yes** to confirm the changes.

Save File Path of Do Not Call List Import File

Many countries require phone solicitors to maintain do not call lists. A Do Not Call (DNC) list ensures that your contact center does not call those customers who request that you do not contact them.

The Do Not Call list is a list of phone numbers that are identified as off-limits for outbound calling. This list can include numbers from a national DNC list and numbers from customers who have directly requested that you not contact them. Outbound Campaigns do not dial entries in the Do Not Call list even if they are included in a contact list. The DNC list is shared across all campaigns and contains only phone numbers.

Before you begin:

1. Using a text editor, create a text file to contain the "Do Not Call" phone numbers.
2. For each "Do Not Call" entry, enter a phone number of up to 20 characters on a new line.

   The following is an example of a Do Not Call list:

   ```
   2225554444
   2225556666
   2225559999
   ```

3. Save the text file to the path that is accessible from the logger.

Procedure

Step 1 In Unified CCE Administration, choose **Organization** > **Campaigns** to open the **Campaigns** page.

Step 2 Click the **Do Not Call - Settings** link.
The **Do Not Call - Settings** pop-up window appears.

Step 3 In the **File Path with Name** field, you must enter the DNC list import file path on the logger or the path accessible from the logger.

Step 4 Click **Save**.
The solution import the DNC phone numbers to Do_Not_Call table in BA database. The name of DNC list import file is renamed after the successful import.

Note On the **Campaigns** page, you can save only one DNC list import file path at a time.

The campaign validates that a number in the dialing list is not in the Do Not Call list before sending it to a dialer. The solution checks the list at the last minute before placing the call. You can update a Do Not Call list while a campaign is running.

To edit the DNC phone numbers import file path:

1. Click the **Do Not Call - Settings** link. The solution displays the existing file path of the DNC list import file in the **File Path with Name** field.
2. Enter the file path of the new or updated DNC list import file in the **File Path with Name** field.
3. (Optional) Check the **Delete existing "Do Not Call" Phone Numbers** check box to delete the existing phone numbers from the Do_Not_Call table.

   If this check box is unchecked, the existing DNC phone numbers are appended to the new or updated DNC phone numbers in the Do_Not_Call table.
4. Click **Save**.

Business Hours

Business Hours

Business hours are the working hours during which you conduct business. You can create and modify business hours and set weekly and daily schedules for each business hour. You can create different business hour schedules for regular working days and holidays. You can also open or close the business hours if there is an emergency.

You can define the status reasons for business hours and assign codes for each status reason. Status reason is required when you force open or force close a business hour, and when you add special hours and holidays.

Search for Business Hours

The Search field on the Business Hours page offers an advanced and flexible search.

Click the + icon on the Search field to open a popup window, where you can:

- Enter a business hour name or description to search for that string.
- Select **Globals and Departments** or **Departments only** to enable an input field where you can enter a space-separated list of department names. (Departments is an OR search.)

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

Add and Maintain Business Hours

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours**.

Step 2 On the **Business Hours** page, click **New** to open the **New Business Hours** page.

Step 3 Complete the following information on the **General** tab and click **Save**.

Field	Required?	Description
Status	-	Select one of the following statuses for the business hour: • **Open/Closed as per Business Calendar** • **Force Open** • **Force Close**
Status Reason	Yes, if the status is Force Open or Force Close.	This field is enabled only if the status is Force Open or Force Close. Search and select a status reason for the business hour.
Name	Yes	Enter a unique name for the business hour. Maximum length is 32 characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric.
Description	No	Enter a description of the business hour.
Time Zone	Yes	Select a time zone of the business hour from the drop-down list.
Department	-	Search and select a department to associate with the business hour. Default is Global. **Note** This is applicable for Packaged CCE deployment only.

Step 4 Click the **Regular Hours** tab and complete the following information:

- Select one of the following **Business Hour Type**:
  - **24x7**: Always open. You cannot customize the working hours.
  - **Custom**: You can customize the working hours.
- If you select **Custom**, enable at least one business day and select the **Start Time** and **End Time**.

Step 5 Click the **Special Hours & Holiday** tab. You can either add or import special hours and holidays.

Step 6 Click **Add** to open the **Add Special Hours & Holiday** popup window. Complete the following information:

Field	Required?	Description
Date	Yes	Select a date from the calendar.

Field	Required?	Description
Description	No	Enter a description for the special hour.
Status	-	Select a status. If the status is **Open**, the **Start Time** and **End Time** fields are enabled.
Start Time	Yes, if status is Open.	Select a start time for the special hour.
End Time	Yes, if status is Open.	Select an end time for the special hour.
Duration	-	Displays the duration of the special hour.
Status Reason	Yes	Search and select a status reason.

Step 7 Click **Save** to add the special hours and holidays.

Step 8 To import special hours and holidays, follow these steps.

a) Click **Import** to open the **Import Special Hours and Holidays** pop-up window.

b) Click the download icon to download the Special Hours & Holidays template. Use this template to enter the special hours and holidays.

c) Click **Choose File** and browse to the special hours and holidays file. Click**Import** to upload the file.

Note The file must contain at least one special hour and holiday.

The file must be in CSV format with a file extension as .txt or .csv.

Step 9 Click **Export** to download the special hours and holidays in .csv format.

Step 10 Click **Save**.

Note The imported business hours overwrites the existing ones.

Add Status Reasons

This procedure explains how to add and maintain status reasons for business hours.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours** > **Status Reasons**.

Step 2 Click **Add** to open the **Add Status Reason** popup window.

Step 3 Enter the Status Reason. Maximum length is 255 characters.

Step 4 Enter a unique Reason Code. Range is 1001 to 65535. Codes 1 to 1000 are reserved as system-defined reason codes.

Step 5 Click **Save**.

To add more status reasons, repeat steps from 2 to 5.

Step 6 Click **Done** to return to the List window.

Edit Status for Multiple Business Hours

Perform the following steps to edit the status of multiple business hours at once.

Procedure

Step 1 On the **Business Hours** page, select two or more business hours to edit.
Step 2 Choose **Edit** > **Status** to open the **Edit Business Hours** page.
Step 3 Check the **Status** check box and select the required status.
Step 4 If you select the status as **Force Open** or **Force Close**, search and select a **Status Reason**.
Step 5 Click **Save**.

Edit Schedule for Multiple Business Hours

Perform the following steps to edit schedules of multiple business hours at once.

Procedure

Step 1 On the **Business Hours** page, select two or more business hours to edit.
Step 2 Choose **Edit** > **Schedule** to open the **Edit Business Hours** page.
Step 3 Check the **Time Zone** check box and the select the required time zone from the drop-down list.
Step 4 Check the **Type** check box and select the required business hour type.
Step 5 If you select **Custom**, enable atleast one business day and select the **Start Time** and **End Time**.
Step 6 Click **Save**.

Desktop Settings

Resources

Resources

The **Resources** page allows you to configure resources for the teams. In Unified CCE Administration, choose **Desktop** > **Resources** to open the **Resources** page. You can select a site from the **Site** drop-down list. By default **Main** is selected for Packaged CCE 2000 Agents deployment.

The Packaged CCE 4000 Agents or 12000 Agents deployment type provides an option to select a peripheral set that includes the Cisco Finesse component configured. For more information to add peripheral sets to a site, see Add and Maintain Peripheral Set.

After you select a site, select a peripheral set from the **Peripheral Set** drop-down list. The drop-down list includes the peripheral sets configured for the selected site.

This page contains the following tabs that you click to configure the respective resources:

- **Call Variables Layout:** Manage the call variables and (Extended Call Context ECC) variables that appear on the agent desktop call control gadget.
- **Desktop Layout:** Make changes to the default desktop layout for agents and supervisors.
- **Phone Books:** Add, edit, or delete phone books or phone book contacts.
- **Workflows:** Create and manage workflows and workflow actions.

The resources that you configure are case-sensitive. For example, you can create two workflows named WORKFLOW and workflow or two phone books named BOOK and book.

Manage Call Variables Layout

You can use the Call Variables Layouts gadget to define how call variables appear on the Finesse agent desktop. You can configure up to 200 unique Call Variables Layouts (one default layout and 199 custom layouts). As part of this functionality:

- Each layout has a name (required) and description (optional).
- After an upgrade from a release earlier than Cisco Finesse Release 11.0, Finesse migrates the previously configured default layout and assigns it the default name (Default Layout) and description (Layout used when no other layout matches the user layout Custom/ECC Variable).
- You can change the name and description of the default Call Variables Layout.
- You cannot delete the default Call Variables Layout.
- Finesse appends *(Default)* to the name of the default Call Variables Layout.
- To display a custom Call Variables Layout, in the Unified CCE routing script set the user.Layout ECC variable to the name of a configured Call Variables Layout. In this case, if no custom layouts match the user.Layout value (or no custom layouts are configured), the Finesse displays the default layout.
- Finesse retains the custom layout as specified by the user.Layout ECC variable on CTI server failover. During PG failover, Finesse changes the active call layout to the default layout while retaining the call variables and time indicators.

Call Variables

Each Call Variables Layout supports one variable in the header of the call control gadget and up to a total of 20 variables in two columns below the header (up to 10 in each column). You can use call variables, Extended Call Context (ECC) variables, or the following Outbound Option ECC variables:

- BACampaign
- BAAccountNumber
- BAResponse

- BAStatus
- BADialedListID
- BATimeZone
- BABuddyName

Columns can be empty.

The administrator can include the following additional fields in the Call Variables Layout. These variables appear as a drop-down list in the call variable gadget which the admin can assign to a layout.

- queueNumber
- queueName
- callKeyCallId
- callKeyPrefix
- callKeySequenceNum
- wrapUpReason

Note The callKeyPrefix indicates the day when the call was routed.

The callKeyCallId indicates the unique number for the call routed on that day.

To uniquely locate the call in Unified CCE database records, concatenate the two variables callKeyPrefix and callKeyCallId.

To enable Outbound Option data to appear in Cisco Finesse, the administrator must edit the Default Layout to include some or all Outbound Option variables.

Configure Call Variables Layouts

Procedure

Step 1 From the Call Variables Layouts gadget:

- Click **New** to create a new Call Variables Layout.
- Choose a layout from the list and click **Edit** to modify an existing Call Variables Layout (or click **Delete** to remove it).

Step 2 Under **Create New Layout** (or under Edit <layout name> when editing an existing layout):

- Enter a name for the Call Variables Layout (maximum 40 characters).
- Enter a description of the Call Variables Layout (maximum 128 characters).

Step 3 Under Call Header Layout:

- Enter the display name that you want to appear in the header of the Call Control gadget on the desktop. For example, Customer Name (maximum 50 characters).
- From the drop-down list, choose the call variable or Outbound Option ECC variable that you want to appear in the header. For example, callVariable3 (maximum 32 characters).

Step 4 In the Call Body Left-Hand Layout and Call Body Right-Hand Layout areas:

a) Click **Add Row** to add a new row (or click the "X" to delete a row).

b) For each row:

- Enter the display name that you want to appear on the desktop. For example, Customer Name (maximum 50 characters).
- Enter the corresponding call variable or Outbound Option ECC variable from the drop-down list (maximum 32 characters).

Step 5 Select up to five call variables using the check box. The selected call variables are displayed in agent call popover and supervisor active call details.

Note If you do not select any call variables, the first two call variables from the Call Body Left-Hand layout area will be displayed in the agent call popover and supervisor active call details. If there are no call variables in the Left-hand layout area, then the call variables in the Right-Hand Layout will be selected.

Step 6 Click **Save** to save the changes, or **Cancel** to discard the changes.

Note When you modify the Call Variables Layout of the agent desktop, the changes you make take effect after three seconds. However, agents or supervisors who are signed in when the changes are made must sign out and sign back in to see those changes reflected on their desktops.

Step 7 To view the latest configured Call Variables Layout, click **Refresh** from the Call Variables Layouts gadget.

Add ECC Variables to Call Variables Layout

Procedure

Step 1 In the header or the row where you want the ECC variable to appear, from the Variable drop-down list, choose **Custom**.

Step 2 In the Custom/ECC Variable Name field, enter the name of the ECC variable you want to appear on the agent desktop.

Step 3 Click **Set**.

The ECC variable now appears in the Variable drop-down list for selection.

Assign Call Variables Layouts

Procedure

Step 1 In CCE Configuration Manager, create an ECC variable called **user.Layout** in the Expanded Call Variable list.

Note If a user.layout and a user.Layout are specified, Finesse will prioritize user.layout over user.Layout. If the layout specified in the user.Layout or user.layout is not found, Finesse uses the Default layout.

Step 2 Add **user.Layout** to the CCE routing script. Use a Set Variable node in an appropriate place in the script to set the value of user.Layout to the name of the call variables layout to display. The layout name should match the name of a call variables layout that was created on the Call Variables Layout tab.

Manipulate Call Variables Layouts with a Workflow

You can manipulate the call variables layout that an agent sees when a call is answered by using a workflow. To do so, configure an HTTP Request workflow action and set the value of the ECC variable user. Layout to the name of the custom layout to display.

Manage Desktop Layouts

You can define the layout of the Finesse desktop on the **Desktop Layouts** tab.

Important Requirements, such as processor speed and RAM, for clients accessing the Finesse desktop can vary. Desktops that receive events for more than one agent (such as agent and supervisor desktops running Live Data reports that contain information about other agents and skill groups) require more processing power than desktops that receive events for a single agent.

Factors that determine how much power is required for the client include, but are not limited to, the following:

- Contact center traffic
- Additional integrated gadgets in the desktop (such as Live Data reports or third-party gadgets)
- Other applications that run on the client and share resources with the Finesse desktop

Gadgets and Components

Gadgets

Cisco Finesse is an OpenSocial gadget, which is an XML document that defines metadata for an OpenSocial Gadget container. The gadgets are applications that are placed within the Cisco Finesse desktop. This helps administrator to provide access to the contact center agents for all the applications that is required to service calls inside a single application.

Cisco Finesse comes with default gadgets such as, the team performance gadget, call control gadget, and call popover. JavaScript library is available for any customers with specific requirements that are not available out of the box.

Gadgets are listed in the desktop layout using the <gadget> tag.

Note Finesse Desktop is tested to perform well with an average of 20 gadgets per Desktop (across all tabs), over a sign in period of 8 minutes for 2000 users (agents and supervisors). When you increase the total number of gadgets that are configured on the Desktop, the CPU consumption marginally increases during users sign in. When all the configured gadgets are enabled for all the users, it impacts the Finesse server. Higher number of gadgets will also need more browser memory and network bandwidth.

If considerably larger number of gadgets are configured or if more users sign in (more than the tested number of users) in a short time frame, you must monitor the CPU consumption and network bandwidth during users sign in and ensure that the end-point devices have enough memory.

Failover uses optimization to sign in the users quickly and is not considered the same as a new browser sign in.

Third-party gadgets are hosted on the Cisco Finesse server using the `3rdpartygadget` web application or on an external web server. Gadgets can make REST requests to services hosted on external servers using the Cisco Finesse JavaScript Library API. To avoid browser cross-origin issues, REST requests are proxied through the backend Shindig web application. Third-party gadgets must implement their own authentication mechanisms for third-party REST services.

For more information about gadgets, see https://developer.cisco.com/docs/finesse/.

Components

Components are simple scripts that are loaded into the desktop directly at predefined positions as directed by the layout, without an enclosing frame and its document.

Components are introduced in the desktop to overcome a few rendering limitations and performance considerations inherent to gadgets.

The <component> tag lists the components in the desktop layout. Currently, the layout validations prevent creating custom components. Hence, default components are allowed in the desktop layouts. The default desktop functionalities are currently registered as components to provide flexibility and to reduce the load on the server.

Finesse Desktop Layout XML

The Finesse Layout XML defines the layout of the Finesse desktop, and the gadgets and components displayed on the desktop.

Use the Desktop Layout gadget to upload an XML layout file to define the layout of the Finesse desktop for agents and supervisors.

To configure Live Data, see Configure Live Data Reports with Multiple Views, on page 145.

Actions on the **Desktop Layouts** gadget are as follows:

- **Finesse Default Layout XML** - Expands to show the layout XML for the default Finesse desktop.
- **Restore Default Layout** - Restores the Cisco Finesse desktop to the default layout.

- **Save** - Saves your configuration changes.
- **Revert** - Retrieves and applies the most recently saved desktop layout.

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 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 2 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 3 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 4 Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.

Step 5 Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.

Step 6 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.

Configure Live Data Reports with Multiple Views

Cisco Unified Intelligence Center allows you to display multiple Live Data reports or views on a single gadget. Agents can select the desired view to display from a drop-down list on the gadget toolbar, which lists up to five report views in *Report Name* - *View Name* format.

This procedure describes how to add multiple Live Data views to the Finesse desktop layout using the viewId_n and filterId_n keys. You can specify up to five report views to appear in your gadget. The first view among the five is the default view. There is no defined order for how the remaining views are displayed.

Finesse still supports the display of a single gadget using a single viewId. However, if you specify the single viewId along with multiple viewId_n keys, the multiple views are used and the single viewId is ignored.

Note To make sure the modified gadget renders in the Finesse desktop, you must give the appropriate permission for that report in Unified Intelligence Center.

Procedure

Step 1 For each report or view that you want to include in the gadget, obtain the associated viewId from the permalink for the view:

a) In Unified Intelligence Center, in Edit view of the report, select the desired view then click **Links**.

The HTML Link field displays the permalink of the customized report.

b) Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor, and then copy the viewID value from the permalink and save it.

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 2 From the Finesse default layout XML, copy the gadget URL for one of the Live Data reports and paste it into a text editor.

Example:

Copy the URL for the Agent Skill Group for HTTPS from the default layout XML and paste it into a text editor:

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

Step 3 To update the URL to refer to a different report view, populate the viewId_1 value (after the equal sign) with the desired viewId obtained in step 1.

Example:

The following shows the URL updated with the example viewId copied from step 1.

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

Step 4 For each additional view you want to include:

a) At the end of the URL, copy and paste the viewId_1 and agentId_1 strings with a leading ampersand.

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName</gadget>
```

b) Update the copied viewId_1 and filterId_1 in the URL to the next available integer (in this example, viewId_2 and filterId_2).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_2=5C90012F10000140000000830A4E5B33&filterId_2=agent.id=CL%20teamName</gadget>
```

c) Populate the copied viewId value (after the equal sign) with the value defined in the permalink for the desired report (in this example, `99E6C8E210000141000000D80A0006C4`).

Example:

```
<gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId_1=5C90012F10000140000000830A4E5B33&filterId_1=agent.id=CL%20teamName&
viewId_2=99E6C8E210000141000000D80A0006C4&filterId_2=agent.id=CL%20teamName</gadget>
```

d) Make sure that the filterId value matches the type required by the report type, as follows:

- Agent Reports: filterId_*N*=agent.id=CL%20teamName
- Agent Skill Group Reports: filterId_*N*=agent.id=CL%20teamName
- Skill Group Reports: filterId_*N*=skillGroup.id=CL%20teamName
- Precision Queue Reports: filterId_*N*=precisionQueue.id=CL%20teamName

Step 5 Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

Step 6 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.

Default Layout XML

The Cisco Finesse default desktop layout XML for Unified CCE and Packaged CCE contains optional gadgets and notes. The notes describe how to modify the layout for your deployment type.

Optional Live Data gadgets in the layout XML are commented out. After you install and configure Live Data, remove the comment tags from the reports that you want to appear on the desktop.

Following are the updates available in the default layout XML for Cisco Finesse desktop:

- Horizontal Header is available in the layout configuration and the Header can be customized.
- Title and Logo of Cisco Finesse desktop can be customized.
- Desktop Chat, TeamMessage, Dialer, Agent Identity, and Non-Voice State Control are added as part of the header component.

  For upgraded layouts, TeamMessage and Desktop Chat will not appear by default. The XML must be copied from the default layout and added to the respective custom layouts. See *Cisco Cisco Finesse Installation & Upgrade Guide*.
- Vertical tabs in Cisco Finesse desktop are moved to collapsible left navigation bar for which the icons can be customized.
- Support for inbuilt java script components has been added.
- The **ID** attribute (optional) is the ID of the HTML DOM element used to display the gadget or component. The ID should start with an alphabet and can contain alphanumeric characters along with hyphen(-) and underscore(_). It can be set through the Cisco Finesse Administrative portal and has to be unique across components and gadgets.
- The **managedBy** attribute (optional) for Live Data gadgets defines the gadgets which manage these Live Data gadgets. The value of **managedBy** attribute for Live Data gadgets is **team-performance**. This means that the rendering of the gadget is managed by the Team Performance gadget. These gadgets are not rendered by default, but will be rendered when the options Show State History and Show Call History are selected in the Team Performance gadget.

  For upgraded layouts, the **managedBy** attribute will be introduced, and will have the value of the **ID** of the Team Performance gadget in the same tab. If there are multiple instances of Team Performance gadgets and Live Data gadget pairs, they will be associated in that order. If the **ID** of the Team Performance gadget is changed, the value of the **managedBy** attribute should also be updated to reflect the same **ID** for the Live Data gadgets. Otherwise, the Team Performance gadget instance will not show its respective Live Data gadgets.
- The **Hidden** attribute (optional) is used to support headless gadgets. When an attribute is set to hidden="true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".

- **maxRows** is changed from being a query parameter to an attribute.

  Example of **maxRows** being a query parameter:

  ```
  <gadget id="team-performance">/desktop/scripts/js/teamPerformance.js?maxRows=5</gadget>
  ```

  Example of **maxRows** being an attribute:

  ```
  <gadget id="team-performance" maxRows="5">/desktop/scripts/js/teamPerformance.js</gadget>
  ```

  During an upgrade it will be removed from the URL of the team performance gadget and added as an attribute. The **maxRows** attribute (optional) is used to adjust the height of the Team Performance gadget. If there are multiple instances of the Team Performance gadget, each instance height can be set by using this attribute. During an upgrade the height of the team performance gadget will be retained. By default the **maxRows** attribute value is set to 10 rows.

If any changes are made to the component IDs or URLs in the default XML layout, the following features may not work as expected.

Note that the components can be rearranged in any order to show on the Cisco Finesse desktop.

Feature	Component ID	URL
Title and Logo	cd-logo	<url>/desktop/scripts/js/logo.js</url>
Voice State Control	agent-voice-state	<url>/desktop/scripts/js/agentvoicestate.component.js</url>
Non-voice state control	nonvoice-state-menu	<url>/desktop/scripts/js/nonvoice-state-menu.component.js</url>
TeamMessage	broadcastmessagepopover	<url>/desktop/scripts/js/teammessage.component.js</url>
Desktop Chat	chat	<url>/desktop/scripts/js/chat.component.js</url>
Dialer	make-new-call-component	<url>/desktop/scripts/js/makenewcall.component.js</url>
Agent identity	identity-component	<url>/desktop/scripts/js/identity-component.js</url>

Update Default Desktop Layout

When you modify the layout of the Finesse desktop, it can take up to 120 seconds to reflect the changes. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflecting on the desktop.

Note The call control gadget is only supported at the page level. You must ensure that the call control gadget (<gadget>/desktop/scripts/js/callcontrol.js</gadget>) is placed within the <page></page> tag for it to work correctly. Don't place this gadget within a <tab></tab> tag.

The version tag of Desktop Layout XML can’t be edited.

For the changes to take effect, refresh the page, or sign out and sign in again into Cisco Finesse.

To modify the Live Data gadget, see Modify Live Data Stock Reports for Finesse, on page 144.

Procedure

Step 1 Click **Desktop Layout**.

Step 2 In the Finesse Layout XML area, make changes to the XML as required.

Example:

If you want to add a new tab called Reports, add the following XML within the tabs tags under the <role>Agent</role> tag:

```
<tab>
   <id>reports</id>
   <icon>Reports</icon>
   <label>Reports</label>
</tab>
```

If you want to add this tab to the supervisor desktop, add the XML within the tabs tags under the <role>Supervisor</role> tag.

To add a gadget to a tab, add the XML for the gadget within the gadgets tag for that tab.

```
<gadgets>
<gadget>http://<ipAddress>/gadgets/<gadgetname>.xml</gadget>
</gadgets>
```

Replace <ipAddress> with the IP address of the server where the gadget resides.

If you want to add multiple columns to a tab on the Finesse desktop, add the gadgets for each column within the columns tags for that tab. You can have up to four columns on a tab.

```
<tabs>
    <tab>
        <id>home</id>
        <icon>home</icon>
        <label>finesse.container.tabs.agent.homeLabel</label>
        <columns>
            <column>
                <gadgets>
                    <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
                </gadgets>
            </column>
        </columns>
    </tab>
    <tab>
        <id>myHistory</id>
        <icon>history</icon>
        <label>finesse.container.tabs.agent.myHistoryLabel</label>
        <columns>
            <column>
                <!-- The following gadgets are used for viewing the call history
and state history of an agent. -->
            </column>
        </columns>
    </tab>
    <tab>
        <id>manageCustomer</id>
        <icon>profile-settings</icon>
        <label>finesse.container.tabs.agent.manageCustomerLabel</label>
        <gadgets>
            <gadget>/3rdpartygadget/files/FinextGadget.xml</gadget>
```

```
        </gadgets>
    </tab>
```

Step 3 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 many 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.

Finesse validates the XML file to ensure that it's valid XML syntax and conforms to the Finesse schema.

Step 4 After you save your changes, if you want to revert to the last saved desktop layout, click **Revert**. If you want to revert to the default desktop layout, click **Restore Default Layout**.

Note During upgrade, any changes made to the Cisco Finesse Default Layout won't be updated. Click on **Restore Default Layout** to get the latest changes.

Horizontal Header

The Horizontal Header on the Finesse desktop has the following components from left to right. All these components can be removed and replaced with custom gadgets as required.

- **Logo:** Default is Cisco logo. Can be customized.
- **Product Name:** Default is Cisco Finesse. Can be customized.
- **Agent State for Voice:** Displays agent state for voice call.
- **Agent State for Digital Channels:** Displays agent state for digital channels.
- **Dialer Component:** Agent can make a new call.
- **Identity Component:** Displays agent name and signout functionality with reason codes.

Note The sum of widths set for all gadgets and components in the header (inside right aligned columns and left aligned colums) should not exceed the total header width. If it exceeds the header width, some of the gadgets/components will not be visible.

Customize Title and Logo in the Header

You can customize the title and logo displayed on the Finesse desktop:

Procedure

Step 1 Click **Desktop Layout**.

Step 2 Enter the product name in the config value tag with title key.

Step 3 Upload the logo file just like any third-party gadget.

For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.

Step 4 Enter the URL of the logo file in the config value tag with logo key.

Example:

```
<configs>
        <!-- The Title for the application which can be customised.-->
<config value="product.full-name" Key="title"/>
     <!-- The logo file for the application-->
     <!--<config key="logo" value="/3rdpartygadgets/<some_sample_image>"/-->
</configs>
```

The customized logo and product name is displayed on the Finesse desktop.

Note The file size that can be uploaded for the logo must be kept within 40 pixels. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

alternateHosts Configuration

The <gadget> element in the Finesse Layout XML provides an attribute to specify alternate hosts from which the gadget can be loaded. This allows the Cisco Finesse desktop to load the gadget using a different host if the primary server is unavailable.

The **alternateHosts** attribute contains a comma-separated list of FQDNs that will be used if the primary-host-FQDN is unavailable.

```
<gadget alternateHosts="host1,host2,host3,...">
         https://<primary-host-FQDN>/<gadget-URL>
    </gadget>
```

The **alternateHosts** attribute is only applicable for gadgets with an absolute URL. That is URLs containing the FQDN of a host, an optional port, and the complete URL path to the gadget. For example: <gadget alternateHosts="host1,host2">*https://primary host/relative_path*</gadget>

If loading the gadget from the primary-host fails, the Cisco Finesse container attempts to load the gadget from the alternate hosts in the order specified in the **alternateHosts** attribute.

The Cisco Finesse desktop may fail to load the gadget even if some of the hosts are reachable. In such cases, refresh the Cisco Finesse desktop.

When the gadget is specified with a relative URL, for example: <*gadget*>*/3rdpartygadgets/relative_path*</*gadget*>, the **alternateHosts** attribute does not apply and is ignored by the Cisco Finesse desktop.

Note If the host serving the gadget fails after the Cisco Finesse desktop was successfully loaded, the desktop must be refreshed in order to load the gadget from an alternate host. The gadget does not implement its own failover mechanism.

Headless Gadget Configuration

Headless gadgets are gadgets which do not need a display space, but can be loaded and run like a background task in the browser. The **Hidden** attribute (optional) is used to support headless gadgets in the layout XML. When an attribute is set to "hidden=true", then the gadget is loaded by the container, but will not be displayed. The default value set for the attribute is "false".

Customize Icons in Left Navigation Bar

You can add icons (both custom and inbuilt) to the collapsible left navigation bar of the Finesse desktop:

Procedure

Step 1 Click **Desktop Layout**.

Step 2 Enter name of the gadget or component in the id tag.

Step 3 Enter the value of the icon in the icon tag.

Step 4 Upload the icon file just like any third-party gadget.

For more information, see section *Upload Third-Party Gadgets* in *Cisco Finesse Admin Guide*.

Note When adding a custom icon, provide the path in the icon tag and if you are adding an inbuilt icon, provide the icon value in the icon tag

Example:

Note The file size that can be uploaded in the left navigation bar as custom icons is 25 pixels by 25 pixels. The maximum width of the tab title in the left navigation bar must be 80 pixels or less. The file types supported are .svg, .png, .gif, and .jpeg/jpg.

XML Schema Definition

You must ensure that the XML uploaded conforms to the XML schema definition for Finesse. The XML schema definition for Finesse is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.cisco.com/vtg/finesse" targetNamespace="http://www.cisco.com/vtg/finesse"
 elementFormDefault="qualified">
   <!-- definition of version element -->
   <xs:element name="version">
      <xs:simpleType>
         <xs:restriction base="xs:double">
            <xs:pattern value="[0-9\.]+" />
         </xs:restriction>
      </xs:simpleType>
   </xs:element>
   <!--  The below elements are for common desktop header and configs -->
   <!--  Copied from:
https://github5.cisco.com/ccbu-shared/common-desktop/blob/master/java/layout-manager/src/main/resources/layoutSchema.xsd
 -->
   <!--  If the common-desktop XSD changes, this too needs to be updated -->
   <!--  Only difference is that, column has been renamed to headercolumn, since column is
 alredy there in finesse desktop layout -->
   <xs:complexType name="configs">
      <xs:sequence>
```

```
            <xs:element name="config" type="config" minOccurs="0" maxOccurs="unbounded" />
         </xs:sequence>
      </xs:complexType>
      <xs:complexType name="config">
         <xs:attribute name="key">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value="[a-zA-Z]*" />
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
         <xs:attribute name="value" type="xs:string" />
      </xs:complexType>
      <xs:complexType name="header">
         <xs:choice>
            <xs:sequence>
               <xs:element name="leftAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
               <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="0"
maxOccurs="1" />
            </xs:sequence>
            <xs:sequence>
               <xs:element name="rightAlignedColumns" type="listOfColumns" minOccurs="1"
maxOccurs="1" />
            </xs:sequence>
         </xs:choice>
      </xs:complexType>
      <xs:complexType name="component">
         <xs:sequence>
            <xs:element name="url" type="xs:string" minOccurs="1" maxOccurs="1" />
            <xs:element name="stylesheet" type="xs:string" minOccurs="0" maxOccurs="1" />
         </xs:sequence>
         <xs:attribute name="id" use="required">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value=".+" />
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
         <xs:attribute name="order">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value="[0-9]{0,10}" />
               </xs:restriction>
            </xs:simpleType>
         </xs:attribute>
      </xs:complexType>
      <xs:complexType name="listOfColumns">
         <xs:sequence>
            <xs:element name="headercolumn" type="headercolumn" minOccurs="1"
maxOccurs="unbounded" />
         </xs:sequence>
      </xs:complexType>
      <xs:complexType name="headercolumn">
         <xs:choice minOccurs="0" maxOccurs="1">
            <xs:element ref="gadget" />
            <xs:element name="component" type="component" />
         </xs:choice>
         <xs:attribute name="width">
            <xs:simpleType>
               <xs:restriction base="xs:string">
                  <xs:pattern value="[0-9]+(px|%)" />
               </xs:restriction>
            </xs:simpleType>
```

```
      </xs:attribute>
   </xs:complexType>
   <!--  The above elements are for common desktop header and configs -->
   <!-- definition of role type -->
   <xs:simpleType name="role">
      <xs:restriction base="xs:string">
         <xs:enumeration value="Agent" />
         <xs:enumeration value="Supervisor" />
         <xs:enumeration value="Admin" />
      </xs:restriction>
   </xs:simpleType>
   <!-- definition of simple elements -->
   <xs:element name="id">
      <xs:simpleType>
         <xs:restriction base="xs:string">
            <xs:pattern value="[a-zA-Z]([-_:\.a-zA-Z0-9])*" />
         </xs:restriction>
      </xs:simpleType>
   </xs:element>
   <xs:element name="label">
      <xs:simpleType>
         <xs:restriction base="xs:string">
            <xs:minLength value="1" />
            <xs:pattern value="[^\r\n]+" />
            <!-- This regex restricts the label string from carriage returns or newline
characters -->
         </xs:restriction>
      </xs:simpleType>
   </xs:element>
   <xs:element name="icon" type="xs:anyURI" />
   <xs:element name="gadget">
      <xs:complexType>
         <xs:simpleContent>
            <xs:extension base="restrictWhiteSpaces">
               <!-- <xs:attribute name="staticMessage" type="xs:string"/> -->
               <xs:attribute name="id">
                  <xs:simpleType>
                     <xs:restriction base="xs:string">
                        <xs:pattern value="[a-zA-Z]([-_a-zA-Z0-9])*" />
                     </xs:restriction>
                  </xs:simpleType>
               </xs:attribute>
               <xs:attribute name="alternateHosts" type="xs:string" />
               <xs:attribute name="managedBy" type="xs:string" />
               <xs:attribute name="hidden" type="xs:boolean" />
            </xs:extension>
         </xs:simpleContent>
      </xs:complexType>
   </xs:element>
   <xs:element name="role" type="role" />
   <xs:element name="gadgets">
      <!-- Grouping of a set of gadgets -->
      <xs:complexType>
         <xs:sequence minOccurs="0" maxOccurs="unbounded">
            <!-- No limit to number of gadget URIs for now -->
            <xs:element ref="gadget" />
            <!-- URI of the gadget xml -->
         </xs:sequence>
      </xs:complexType>
   </xs:element>
   <xs:simpleType name="restrictWhiteSpaces">
      <xs:restriction base="xs:anyURI">
         <xs:minLength value="1" />
         <xs:pattern value="\S+" />
```

```
      <!-- This regex restricts anyURI from containing whitespace within -->
   </xs:restriction>
</xs:simpleType>
<xs:element name="column">
   <!-- Grouping of a set of gadgets within a column -->
   <xs:complexType>
      <xs:sequence minOccurs="0" maxOccurs="unbounded">
         <!-- No limit to number of gadget URIs for now -->
         <xs:element ref="gadgets" />
         <!-- URI of the gadget xml -->
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="columns">
   <!-- Grouping of a set of columns -->
   <xs:complexType>
      <xs:sequence>
         <xs:element ref="column" minOccurs="0" maxOccurs="unbounded" />
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="page">
   <!-- Grouping of a set of persistent gadgets -->
   <xs:complexType>
      <xs:sequence minOccurs="0" maxOccurs="unbounded">
         <!-- No limit to number of gadget URIs for now -->
         <xs:element ref="gadget" />
         <!-- URI of the gadget xml -->
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="tab">
   <xs:complexType>
      <xs:sequence>
         <xs:element ref="id" />
         <!-- Id of the tab selector in the desktop -->
         <xs:element ref="icon" minOccurs="0" maxOccurs="1" />
         <xs:element ref="label" />
         <!-- Label of the tab selector -->
         <xs:choice>
            <xs:element ref="gadgets" minOccurs="0" maxOccurs="1" />
            <xs:element ref="columns" minOccurs="0" maxOccurs="1" />
         </xs:choice>
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="tabs">
   <!-- Grouping of tabs -->
   <xs:complexType>
      <xs:sequence maxOccurs="unbounded">
         <!-- No limit to number of tabs for now -->
         <xs:element ref="tab" />
      </xs:sequence>
   </xs:complexType>
</xs:element>
<xs:element name="layout">
   <xs:complexType>
      <xs:sequence>
         <xs:element ref="role" />
         <!-- Type of the role -->
         <xs:element ref="page" />
         <!-- List of page gadgets -->
         <xs:element ref="tabs" />
         <!-- Grouping of tabs for this particular role -->
```

```
            </xs:sequence>
         </xs:complexType>
      </xs:element>
      <xs:element name="finesseLayout">
         <!-- Layout of the desktop -->
         <xs:complexType>
            <xs:sequence>
               <xs:element ref="version" />
               <xs:element name="configs" type="configs" minOccurs="0" maxOccurs="1" />
               <xs:element name="header" type="header" minOccurs="1" maxOccurs="1" />
               <xs:sequence maxOccurs="3">
                  <!-- only support 3 roles for now -->
                  <xs:element ref="layout" />
               </xs:sequence>
            </xs:sequence>
         </xs:complexType>
      </xs:element>
</xs:schema>
```

Manage Phone Books

On the **Phone Books** section, you can create and manage global and team phonebooks and phonebook contacts. Global phonebooks are available to all agents; team phonebooks are available to agents in that specific team.

The system supports the following number of phone books:

- 10 global phone books
- 300 team phone books

The system supports a total of 50,000 contacts. The total number of contacts per agent across all phone books is limited to 1500.

Use the **Phone Books** gadget to view, add, edit, or delete phone books and phone book contacts. Click the Name or Assign To headers to sort the phone books in ascending or descending order. Click the Last Name, First Name, Number, or Note headers to sort the contacts in ascending or descending order.

The following table describes the fields on the **Phone Books** gadget.

Field	Explanation
Name	The name of the phone book. The name must be unique, and can be a maximum length of 64 alphanumeric characters.
Assign To	Indicates if the phone book is global (All Users) or team (Teams).
Last Name	The last name of a contact. The last name can be a maximum length of 128 characters. This field is optional.
First Name	The first name of a contact. The first name can be a maximum length of 128 characters. This field is optional.
Number	The phone number for the contact. The phone number can be 1-32 characters long and cannot be blank.
Note	Optional text that describes the contact. The note can be a maximum length of 128 characters.

Actions on the Phone Books gadget:

- **New:** Add a new phone book or contact
- **Edit:** Edit an existing phone book or contact
- **Delete:** Delete a phone book or contact
- **Refresh:** Reload the list of phone books or contacts from the server
- **Import:** Import a list of contacts to the phone book
- **Export:** Export a list of contacts from the phone book

Add Phone Book

Procedure

Step 1 In the **Phone Books** gadget, click **New**.

The New Phone Book area appears.

Step 2 In the **Name** field, enter a name for the phone book.

Note Phone book names can be a maximum of 64 characters.

Step 3 From the **Assign To** drop-down, select **All Users** if the phone book is global or **Teams** if the phone book is available to specified teams.

Step 4 Click **Save**.

Edit Phone Book

Procedure

Step 1 In the **Phone Books** gadget, select the phone book you want to edit.

Step 2 Click **Edit**.

Step 3 In the **Name** field, enter the new name for the phone book. If you want to change who can access the phone book, in the **Assign To** drop-down, choose **All Users** or **Teams**.

Step 4 Click **Save**.

If you change the Assign To field from Teams to All Users, click **`Yes`** to confirm the change.

Delete Phone Book

Procedure

Step 1 In the **Phone Books** gadget, select the phone book that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected phone book.

Add Contact

Procedure

Step 1 In the **Phone Books** gadget, select the phone book to which you want to add a contact.

The List of Contacts for <phone book name> area appears.

Step 2 Click **New**.

Step 3 Complete the fields. The First Name, Last Name, and Note fields are optional and have a maximum length of 128 characters. The Number field is required and has a maximum length of 32 characters.

Step 4 Click **Save**.

Edit Contact

Procedure

Step 1 In the **Phone Books** gadget, select the phone book that contains the contact you want to edit.

The List of Contacts for <phone book name> area appears.

Step 2 Select the contact you want to edit.

Step 3 Click **Edit**.

Step 4 Edit the fields that you want to change. The First Name, Last Name, and Note fields are optional and have a maximum of 128 characters. The Number field is required and has a maximum of 32 characters.

Step 5 Click **Save**.

Delete Contact

Procedure

Step 1 In the **Phone Books** gadget, select the phone book that contains the contact you want to delete.

The List of Contacts for <phone book name> area appears.

Step 2 Select the contact that you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Yes** to confirm the deletion of the selected contact.

Import Contacts

The Import function allows you to replace all the contacts in a phone book with a new list of contacts, or to populate a new phone book with contacts.

The import list must be in the specified comma separated values (CSV) format, and can contain a maximum of 1500 contacts. Import lists that contain more than 1500 contacts are rejected with an error message.

The CSV file contains the fields described in the following table:

Field	Max Length	Can Be Blank?	Permitted Characters
First Name	128	Yes	Alphanumeric characters **Note** The CSV file that contains the contacts to import must use Latin encoding.
Last Name	128	Yes	
Phone Number	32	No	
Notes	128	Yes	

The following is an example of a phone book CSV file:

```
"First Name","Last Name","Phone Number","Notes"
"Amanda","Cohen","6511234",""
"Nicholas","Knight","612-555-1228","Sales"
"Natalie","Lambert","952-555-9876","Benefits"
"Joseph","Stonetree","651-555-7612","Manager"
```

A phone book CSV file must conform to this format and include the headers in the first line. During import, the file is scanned for illegal characters. If any are found, they are replaced with question marks.

Note Exported CSV files always show each field enclosed in double quotes to ensure that any commas or double quotes that are part of the actual filed data are not mistaken for field delimiters. If your data does not include these characters, you can omit the double quotes in files you prepare for importing.

Procedure

Step 1 In the **Phone Books** gadget, select the phone book into which you want to import a list of contacts.

Step 2 Click **Import**.

Step 3 Click **Browse** and navigate to the location of the CSV file containing the contacts you want to import.

Note The CSV file must use Latin encoding.

Step 4 Click **OK**.

Export Contacts

The Export function allows you to extract a list of contacts from an existing phone book. The exported list is saved in CSV format.

Procedure

Step 1 In the **Phone Books** gadget, select the phone book that contains the contacts you want to export.

Step 2 Click **Export**.

Step 3 Click **Open** to open the CSV file in Excel, or click the **Save** drop-down list and choose **Save**, **Save as**, or **Save and open**.

Step 4 A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.

Step 5 A message appears that gives you the option to view the downloaded file, open the folder into which the download was saved, view the Internet Explorer View Downloads window, or dismiss the message without viewing the file.

Manage Workflows

On the **Workflows** tab, you can create and manage workflows and workflow actions.

Workflows and Workflow Actions

You can use workflows to automate common repetitive agent tasks. A workflow has a unique name and a helpful description. Use the Manage Workflows and Manage Workflow Actions gadgets to view, add, edit, or delete workflows and workflow actions.

All workflows are team-level workflows. You cannot create a global workflow. If you need a global workflow, create a team workflow and assign it to all teams.

Cisco Finesse supports the following number of workflows and workflow actions:

- 100 workflows per Cisco Finesse system
- 100 actions per Cisco Finesse system
- 20 workflows per team
- Five conditions per workflow
- Five actions per workflow
- Five variables per action

The following fields can be used to configure workflows:

- queueNumber
- queueName
- callKeyCallId
- callKeyPrefix
- callKeySequenceNum
- wrapUpReason

- For Voice - Call variables, Outbound Option variables, queue details, wrap-up reasons, agent details, or team details.
- For Email - Queue name and email attributes like From, To, Cc, Bcc, or Subject.
- For Chat - Queue name, chat type, or system defined customer details as available from the web chat form.

Click the column headers to sort workflows and workflow actions in ascending or descending order.

The following table describes the fields on the Manage Workflows gadget:

Field	Explanation
Name	The name of the workflow must be unique and can have a maximum length of 40 characters.
Description	The description of the workflow can have a maximum length of 128 characters.
Media	The media of the workflow. You can configure the media to Voice and any preferred Digital Channel.

The following table describes the fields on the Manage Workflow Actions gadget:

Field	Explanation
Name	The name of the workflow action must be unique and can have a maximum length of 64 characters.
Type	The type of workflow. Possible values are Browser Pop and HTTP Request.

Actions on the Manage Workflows and Manage Workflow Actions gadgets:

- **New:** Add a new workflow or workflow action
- **Edit:** Edit a workflow or workflow action
- **Delete:** Delete a workflow or workflow action
- **Refresh:** Reload the list of workflows or workflow actions from the server.

You can configure workflow actions to be handled by the Cisco Finesse desktop or in a third-party gadget. A third-party gadget can be designed to handle the action differently than Cisco Finesse does.

Each workflow must contain only one trigger. Triggers are based on Cisco Finesse dialog events.

Note You can configure the trigger only after you select the media.

- Voice dialog events include the following:
  - When a Call arrives
  - When a Call is answered
  - When a Call ends

- When making a Call
- While previewing an Outbound Option call.

- Digital Channels dialog events include the following:
  - When a task is offered
  - When a task is accepted

Note Some solutions such as ECE don't provide a separate accept task functionality. Therefore, the tasks that are offered are auto accepted, which simultaneously generate the **task is accepted** event along with the **task is offered** event. In such scenarios, use only one event (**task is accepted** or **task is offered**) for configuring workflows because there is no difference between these two events.

  - When a task is active
  - When a task is paused
  - When a task is interrupted
  - When a task is closed

The workflow engine uses the following simple logic to determine whether to run a workflow:

Note The workflow logic and examples are similar for all media.

- Its trigger set and conditions are evaluated against each dialog event received.
- The workflow engine processes workflow events for the first call that matches any configured workflow's trigger set and conditions. No other workflows run until this call has ended. If the agent accepts a second call while still on the first call, workflows do not run on the second call even after the first call has ended.
- After a workflow for a particular trigger type (for example, Call Arrives) runs, it never triggers again for the same dialog ID.

The workflow engine caches workflows for an agent when the agent signs in. Workflows do not change for the agent until the agent signs out and signs in again or refreshes the browser.

Note Whenever the browser is refreshed, the workflows that trigger the following events run:

- when a call arrives
- when a call is answered
- when making a call

When an agent refreshes the browser, the workflow engine considers the call as newly arrived or newly made. If an HTTP request action is part of the workflow, the HTTP request is sent when the agent refreshes the browser. Applications that receive the HTTP requests must account for this scenario.

An example of a workflow is a Call Arrival event that triggers an action that collects information from the dialog event (for example, the ANI or customer information) and displays a web page containing customer information.

You can filter trigger events by the value of the data that comes in the event. You can configure a workflow to run if any of the conditions are met or if all the conditions are met.

Individual conditions comprise of the following:

- A piece of event data to be examined. For example, **DNIS** or call variables.
- A comparison between the event data and the values entered (for example **contains**, **is equal to**, **is not equal to**, **begins with**, **ends with**, **is empty**, **is not empty**, and **is in list**).

When the trigger and its conditions are satisfied, a list of actions assigned to the workflow are run. The actions are run in the listed order.

Workflows run only for agents and supervisors who are Cisco Finesse users. The Workflow Engine is a JavaScript library that runs client-side on a per-user basis within the Cisco Finesse desktop application. The desktop retrieves the workflows that are to be run for a user from the server when the user signs in or when the browser is refreshed.

Note Changes made to a workflow or its actions while a user is signed in are not automatically pushed to that user.

It is possible to set workflows, conditions, and actions that are contradictory so that a workflow or action cannot function. Workflows are not validated.

If multiple workflows are configured for a team, the Workflow Engine evaluates them in the configured order. The Workflow Engine ignores workflows with no actions. When the Workflow Engine finds a workflow with a matching trigger for an event and the workflow conditions evaluate to true, that workflow is used, and the subsequent workflows in the list are not evaluated. Workflows with no conditions evaluate to true if the event matches the workflow trigger. All workflows are enabled by default. Only one workflow for a specific user can run at a time.

The Workflow Engine retrieves dialog-based variables that are used in workflow conditions from the dialog that triggered the workflow. If a variable is not found in the dialog, it's value is considered to be empty.

The Workflow Engine runs the actions that are associated with the matched workflow in the order in which they are listed. The Workflow Engine runs actions in a workflow even if the previously run action fails. Failed actions are logged.

The Cisco Finesse server controls the calls that are displayed to the Cisco Finesse user. If the user has multiple calls, the workflow applies only to the first call that matches a trigger. If the first call displayed does not match any triggers but the second call does match a trigger, the Workflow Engine evaluates and processes the triggers for the second call.

A call is considered to be the first displayed call if it is the only call on the Cisco Finesse desktop when it appears. If two calls on a phone are merged (as they are in a conference call), then the first displayed call flag value of the surviving call is used.

If a user has a call and the user refreshes the browser, the Workflow Engine evaluates the call as it is. If the dialog data (call variable values) change, the data may not match the trigger and conditions of the original workflow. The data may match a different workflow or no workflows at all.

If a user has multiple calls and the user refreshes the browser, the Workflow Engine treats the first dialog received from the Cisco Finesse server as the first displayed call. This call may not be the same call that was first displayed before the refreshing the browser. Dialogs received for any other call are ignored because they are not considered as first displayed calls. After refreshing the browser, if dialogs for more than one call are received before the Workflow Engine is loaded, none of the dialogs are evaluated because they are not considered as first displayed calls.

Workflows that are run for both Cisco Finesse agents and supervisors. The team to which the supervisor belongs (as distinguished from the team that the supervisor manages) determines which workflows run for the supervisor. Put the supervisors in their own team to keep agent workflows from being run for them.

Workflow Triggers and Outbound Calls

Note When you create a workflow specifically for Outbound Option calls, add a condition of BAStatus is not empty (except for the Workflow Trigger 'When a call arrives' as BAStatus will be empty at that point of time). This condition ensures that the workflow can distinguish Outbound Option calls from agent-initiated outbound calls.

The following table illustrates when workflows trigger in outbound call scenarios:

Workflow Trigger	Direct Preview Outbound Call	Preview Outbound Call	Progressive/Predictive Outbound Call
While previewing a call	When the agent previews the call (before accepting or rejecting it)	When the agent previews the call (before accepting or rejecting it)	Does not trigger
When a call arrives	Does not trigger	When the agent accepts the call	When the call arrives on the agent desktop
When a call is answered	When the customer answers the call and during failover	When the customer answers the call and during failover	When the customer answers the call
When a call is made	When the customer call is initiated	When the customer call is initiated	When the customer call is initiated, and during failover
When a call ends	When the customer call ends	When the customer call ends	When the customer call ends

Add Browser Pop Workflow Action

The Browser Pop workflow action opens a browser window or tab on the user's desktop when workflow conditions are met.

Note Whether the action opens a new window or tab on the desktop depends on the target user's browser settings.

Procedure

Step 1 In the Workflow Actions gadget, click **New**.

Step 2 In the Name box, enter a name for the action.

Note Workflow action names are limited to 64 characters.

Step 3 From the Type drop-down list, choose **Browser Pop**.

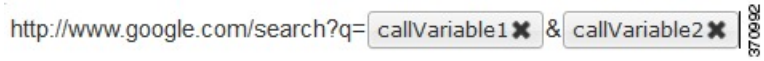
Step 4 From the Handled By drop-down list, choose what will run the action, either the Finesse Desktop or Other (a third-party gadget).

Step 5 In the Window Name box, enter the ID name of the window that is opened. Any action that uses this window name reuses that specific window.

Note Window names are limited to 40 characters, and can be blank. If you leave the window name blank, a new window opens every time the action runs.

Step 6 Enter the URL of the browser window and click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags.

Example:



For every variable you select, you can enter test data in the Sample Data box. A sample URL is automatically built in the Browser URL box below the Sample Data area. To test the URL, click Open to open the URL in your browser.

Note The system does not validate the URL you enter.

Step 7 Click **Save**.

Add HTTP Request Workflow Action

The HTTP Request workflow action makes an HTTP request to an API on behalf of the desktop user.

Procedure

Step 1 In the Workflow Actions area, click **New**.

Step 2 In the Name box, enter a name for the action.

A workflow action name can contain a maximum of 64 characters.

Step 3 From the Type drop-down list, select **HTTP Request**.

Step 4 From the Handled By drop-down list, select what will run the action, the Finesse desktop or Other (a third-party gadget).

Step 5 From the Method drop-down list, select the method to use.

You can select either PUT or POST.

Step 6 From the Location drop-down list, select the location.

If you are making the HTTP request to a Finesse API, select **Finesse**. If you are making a request to any other API, select **Other**.

Step 7 In the Content Type box, enter the content type.

The default content type is application/xml, which is the content type for Finesse APIs. If you are using a different API, enter the content types for that API (for example, application/JSON).

Step 8 In the URL box, enter the URL to which to make the request. To add variables to the URL, click the tag icon at the right of the box and select one or more variables from the drop-down list.

Example:

The following is the URL example for a Finesse API:

Note If you want to make a request to another API, you must enter the entire URL (for example, http://googleapis.com).

You can click the tag icon at the right of the box and select one or more variables from the drop-down list to add tags to the URL. In the preceding example, to add the dialogId, click the tag icon and select dialogId from the list.

Step 9 In the Body box, enter the text for the request. The body must match the content type (for example, if the content types is application/xml, the body must contain XML). To add variables to the body, click the tag icon at the right of the box and select one or more variables from the drop-down list.

Example:

To make an HTTP request to the Dialog - Start a recording API, enter the following into the Body box:

To add the extension, click the tag icon and select extension.

For every variable you add, you can enter test data in the Sample Data box.

Step 10 Click **Save**.

Edit Workflow Action

Procedure

Step 1 In the Workflow Actions gadget, select the action that you want to edit.

Step 2 Click **Edit**.

Step 3 Edit the fields that you want to change.

Step 4 Click **Save**.

Delete Workflow Action

Procedure

Step 1 In the Workflow Actions gadget, select the action that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected action.

Add Workflow

Procedure

Step 1 In the Workflows gadget, click **New**.

Step 2 From the **Choose Media** drop-down, select the media.

Note In case of a voice only configuration, the **Choose Media** drop-down will display only Voice.

Step 3 In the **Name** box, enter the name of the workflow.

Note The name is limited to 40 characters.

Step 4 In the **Description** box, enter a description of the workflow.

Note The description is limited to 128 characters.

Step 5 In the **When to perform Actions** drop-down list, select the event that triggers the workflow.

Note The drop-down actions change depending on the selected media.

Step 6 In the **How to apply Conditions** box, select if all conditions are met, or if any conditions are met, and then click **Add Condition** to add up to five conditions.

Note Variables in the drop-down for conditions are grouped depending on the selected media.

Example:

For example, you can specify that the action is taken when CallVariable 1 equals 123 and CallVariable 2 begins with 2.

Step 7 In the Ordered List of Actions area, click **Add** to open the Add Actions area. Click an action in this area to add it to the Ordered List of Actions.

Step 8 Use the up and down arrows next to the Ordered List of Actions to move actions into the performance order.

Step 9 Click **Save**.

Step 10 Assign the workflow to one or more teams.

Note A workflow does not run until it is assigned to a team.

Edit Workflow

Procedure

Step 1 In the Workflows gadget, select the workflow you want to edit.

Step 2 Click **Edit**.

Note The media for an existing workflow can be changed by editing the workflow.

Step 3 Edit the fields that you want to change.

Step 4 Click **Save**.

Delete Workflow

Procedure

Step 1 In the Workflows gadget, select the workflow that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **Yes** to confirm the deletion of the selected workflow.

Reason Labels

Reason Labels

The Reason Labels feature in Packaged CCE is used to configure the Not Ready, Sign Out, and Wrap-Up reason labels. Agents select the reason on their agent desktops (Cisco Finesse) to provide the work status. Reason label appears in the Unified Intelligence Center reports, and helps to identify the agents' work behavior, for example, if the agent is spending long time in meetings or taking an inappropriate number of breaks, and so on.

The Reason Labels configured in Packaged CCE webadmin appear in the Finesse desktop of all sites in a global deployment.

Supervisors cannot access this Reason Labels feature.

To configure the reason labels, navigate to **Unified CCE Administration** > **Overview** > **Desktop Settings** > **Reason Labels**, or choose **Desktop** > **Reason Labels** from the left navigation.

Note To view the maximum limit for Not Ready reason codes, Sign Out reason codes, and Wrap-up reason labels for the Global and Team Specific reasons, click **Capacity** on the left navigation. For more information, see Capacity Info, on page 242.

The Reason Labels list window has some predefined system reason labels for Not Ready and Sign Out reasons. You cannot delete these system reason labels, however you can modify the label and description. To view the list of system reason codes, see Predefined System Reason Codes, on page 170.

Note After upgrade, the system defined reason labels pre-populate in the Reason Labels List window. However, you must reconfigure all the custom defined reason labels. See Add and Maintain Reason Labels, on page 169

Add and Maintain Reason Labels

This procedure explains how to add a reason label. For information on maintaining reason labels, see Update Objects, on page 4 and Delete Objects, on page 7.

Procedure

Step 1 In **Unified CCE Administration**, choose **Desktop** > **Reason Labels** from the left navigation.

Step 2 Click **New**.

Step 3 Complete the following fields:

Fields	Required?	Description
Type	-	Select a reason type from the drop-down list - **Not Ready**, **Sign Out**, **Wrap-Up**.
Label	Yes	Enter a label for the selected reason type. The field allows maximum of 40 characters. Both alphanumeric and special characters are supported. **Note** Enter unique labels for the Wrap-Up reasons.
Code	Yes	Enter a unique code for the selected reason type. The valid range is from 1 to 65535. **Note** The **Code** field is not available for the **Wrap-Up** reasons.

Fields	Required?	Description
Description	No	Enter a maximum of 255 characters to describe the reason label. See Character Sets.

Step 4 To assign the reason label to one for more teams, select the **Team Specific** option.

Note By default, the **Global** option is selected to make the reason label generic or visible to all teams.

Step 5 Click **Save** to return to the List screen, where a message confirms the successful creation. You can perform the Sort a List, Search a List, and Delete Objects tasks on the List screen.

What to do next

To assign the configured team specific reason labels to one or more teams, navigate to **Organization** > **Teams** (**Team Resources** tab) from the left navigation. For more information, see Add and Maintain Teams , on page 99.

Predefined System Reason Codes

For Not Ready system reason codes and Sign Out system reason codes, only the reason code label can be edited and saved. The Global attribute and system code cannot be modified. In case the system reason code label is modified and you wish to revert to the default label, refer to the following list of predefined system reason codes:

System Reason Code	Reason Label	Reason Label Description
32767	Not Ready - Call Not Answered	Agent state changed because the agent did not answer the call.
32762	Ready - Offhook Not Ready - Offhook	The system issues this reason code in the following scenarios: • When the agent goes off the hook to place a call. If the agent remembers to do this task the corresponding agent-triggered reason code is displayed. If the agent does not remember to do this task, the system issues this reason code. • When the agent is in Ready state and a call is placed from the ACD (Automatic Call Distribution) line, the system issues this reason code.
50001	Logged Out - System Disconnect	The CTI OS client disconnected, logging the agent out.
50002	Logged Out - System Failure	A CTI OS component disconnected, causing the agent to be logged out or set to the Not Ready state. This could be due to closing the agent desktop application, heart beat time out, or a CTI OS Server failure.

50002	Not Ready - Connection Failure	The system issues this reason code when the agent is forcibly logged out in certain cases.
50003	Logged Out - Device Error	Agent was logged out because the Unified CM reported the device out of service.
50004	Logged Out - Inactivity Timeout	Agent was logged out due to agent inactivity as configured in agent desk settings.
50005	Not Ready - Non ACD Busy	For a Unified CCE agent deployment, where the Agent Phone Line Control is enabled in the peripheral and the Non ACD Line Impact is configured to impact agent state, the agent is set to Not Ready while talking on a call on the Non ACD line with this reason code.
50010	Not Ready - Call Overlap	Agent was set to Not Ready state because the agent was routed two consecutive calls that did not arrive.
50020	Logged Out - Queue Change	Agent was logged out when the agent's skill group dynamically changed on the Administration & Data Server.
50030	Logged Out - Device Conflict	If an agent is logged in to a dynamic device target that is using the same dialed number (DN) as the PG static device target, the agent is logged out.
50040	Logged Out - Mobile Agent Call Fail	Mobile agent was logged out because the call failed.
50041	Not Ready - Mobile Call Not Answered	Mobile agent state changed to Not Ready because the call fails when the mobile agent's phone line rings busy.
50042	Logged Out - Mobile Agent Disconnect	Mobile agent was logged out because the phone line disconnected while using nailed connection mode.
65535	Not Ready - System Reinitialized	Agent reinitialized (used if peripheral restarts).
65534	Not Ready - System Reset	PG reset the agent, normally due to a PG failure.
65533	Not Ready - Extension Modified	An administrator modified the agent's extension while the agent was logged in.
20001	Not Ready - Starting Force Logout	Places the agent in the Not Ready state first before forcefully logging them off.
20002	Logged Out - Force Logout	Forces the logout request; for example, when Agent A attempts to log in to Cisco Agent Desktop and Agent B is already logged in under that agent ID, Agent A is asked whether or not to force the login. If Agent A answers yes, Agent B is logged out and Agent A is logged in. Reports then show that Agent B logged out at a certain time with a reason code of 20002 (Agent B was forcibly logged out).

20003	Not Ready - Agent Logout Request	If not already in the Logout state, request is made to place agent in the Not Ready state. Then logout request is made to log agent out.
999	Not Ready - Supervisor Initiated	The system issues this reason code when the agent's state is forcibly changed to Not Ready by the Supervisor.
999	Logged Out - Supervisor Initiated	The system issues this reason code when the agent's state is forcibly changed to Logout by the Supervisor.
255	Logged Out - Connection Failure	The system issues this reason code when the agent is forcibly logged out when there is a connection failure between the Cisco Finesse Desktop and the Cisco Finesse Server.

Desk Settings

Desk Settings

Desk settings are a collection of permissions or characteristics for the agent, such as how and when calls to the agent are redirected, how and when the agent enters various work states, and how requests to the supervisor are handled.

To configure desk settings, go to **Unified CCE Administration** > **Desktop** > **Desk Settings**.

Administrators have unlimited access to Desk Settings configuration. Supervisors cannot access Desk Settings.

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.

Add and Maintain Desk Settings

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Desktop** > **Desk Settings**.

Step 2 Click **New** to open the **New Desk Settings** window.

Step 3 Complete the following fields:

Field	Required?	Description
Name	yes	Enter a unique name that will identify the desk settings, using a maximum of 32 alphanumeric characters.
Description	no	Enter a description for the desk settings.

Logout Inactivity Time	no	Enter the number of seconds an agent can be inactive while in the Not Ready state before the system logs the agent out. This number can be from 10 seconds to 7200 seconds (2 hours). Leave this field blank to disable the timer. For agents who handle both voice and nonvoice tasks in the Cisco Finesse agent desktop, leave this field blank.
Wrapup on Incoming	yes	From the drop-down menu, select **Optional** (the default), **Required**, **Not Allowed**, or **Required with wrap-up data** to indicate whether the agent is allowed or required to enter wrap-up data after an incoming call. A selection of **Optional** means the agent can choose to enter wrap-up data or to answer another call.
Wrapup on Outgoing	yes	From the drop-down menu, select **Optional** (the default), **Required**, or **Not Allowed** to indicate whether the agent is allowed or required to enter wrap-up data after an outgoing call. A selection of **Optional** means the agent can choose to enter wrap-up data or to answer another call.
Wrapup Timer	no	Enter a value in seconds between 1 and 7200 to specify the time within which the agent can enter wrap-up data before being timed out. The default is 7200 seconds.
Supervisor Assist Call Method	no	From the drop-down menu, select either: • **Consultative Call** (default): The caller is aware when the supervisor joins the call. This option is supported in CTI OS and Finesse agent desktops. • **Blind Conference:** The caller is not aware when the supervisor joins the call. This option is supported only in CTI OS agent desktops.
Emergency Call Method	no	From the drop-down menu, select either: • **Consultative Call** (default): The caller is aware when the supervisor joins the call. This option is supported in CTI OS and Finesse agent desktops. • **Blind Conference:** The caller is not aware when the supervisor joins the call. This option is supported only in CTI OS agent desktops.
Agent State after RONA	no	From the drop-down menu select either: • **Not Ready** (default): The agent is set as not ready after RONA. • **Ready**: The agent is set as ready after RONA.

Mobile Agent	no	From the drop-down menu select one of the following: • **Not Allowed**: In this mode, Mobile Agent is not allowed. • **Call by Call**: In this mode, the Mobile Agent's phone is dialed for each incoming call. When the call ends, the Mobile Agent's phone is disconnected before being made ready for the next call. • **Nailed Up**: In this mode, the agent is called at login time and the line stays connected through multiple customer calls. • **Agent Chooses**: In this mode, an agent can select a call delivery mode at login.
Enable mobile agent	no	Unchecked by default. When checked, indicates that the agent is a Mobile Agent who can sign in remotely and take calls from any phone. With this selected, the agent can also sign in as a usual agent.
Require Idle Reason	no	Unchecked by default. When checked, indicates that the agent must enter a reason before entering the Idle state.
Require Logout Reason	no	Unchecked by default. When checked, indicates that the agent must enter a reason before logging out.
Play zip tone	no	Unchecked by default. Checked, will play a zip tone to the agent when call is auto-answered. **Note** Only if the administrator enables the Auto answer option, Play ziptone can be enabled.

Note There is no RONA timer field on the Desk Settings tool. The Requery on No Answer (RONA) timer on the Unified Cisco Unified Voice Portal (CVP) controls the agent desk settings for Packaged CCE.

Step 4 Save the desk settings to return to the List window, where a message confirms the successful creation.

Agent Trace

Agent Trace

Enabling agent trace allows you to track and report on every state an agent passes through. You might enable agent trace if you have concerns about the productivity or performance of one or more agents.

Important Enabling trace can affect system performance, as it requires additional network bandwidth and database space. Typically, you use this feature for short-term tracking of specific agents. The system imposes a configuration limit on the number of agents for whom you can enable trace.

Use this tool to view, add, and remove agents for whom agent trace is enabled.

Add and Maintain Agent Trace

Procedure

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

Step 2 Click the **+** icon to open the **Add Agents with Trace Enabled** popup window. Use the sort and search features to navigate the list.

Step 3 Click one or more agent usernames to give them the trace-enabled status.

Step 4 Close **Add Agents with Trace Enabled** to return to the list.

Step 5 Click **Save** on the List window to confirm the trace status for the agents you added. Click **Revert** before you save to remove an agent from the Trace Enabled list.

Remove Agent Trace

Procedure

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

Step 2 On the **List of Agents with Trace Enabled** list, locate the agent whose trace status you want to remove.

Step 3 Click the **x** icon to clear trace status for that agent.

Step 4 Click **Save** on the List window to confirm the removal. To cancel, click **Revert**.

Call Settings

Route Settings

The **Route Settings** page allows you to configure the initial settings for the call flow.

Media Routing Domains

Media Routing Domains (MRDs) organize how requests for each communication medium, such as voice and email, are routed to agents.

An agent can handle requests from multiple MRDs. For example, an agent can belong to a skill group in an MRD for email and to a skill group in an MRD for voice calls.

Configure at least one MRD for each communication medium your system supports. You do not need to configure an MRD for voice; the Cisco_Voice MRD is built in.

You can add and update only Cisco_Task MRDs using the Unified CCE Administration Media Routing Domain tool.

Note To add or update Multichannel MRDs for Enterprise Chat and Email, use the Configuration Manager Media Routing Domain List tool.

Add and Maintain Media Routing Domains

This procedure explains how to add a Multichannel Media Routing Domain (MRD). For information on maintaining MRDs, see Update Objects and Delete Objects.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings**.
The **Route Settings** window opens that shows the list of configured Media Routing Domains.

Step 2 Click **New**.

Step 3 Complete the following fields:

Field	Description
Type	The read-only type of the Media Routing Domain.
Name	Enter a unique name for the Media Routing Domain.
Description	Enter a description for the Media Routing Domain. See Character Sets.
Service Level Threshold	Enter the maximum time, in seconds, that a customer should wait before being connected with an agent.
Interruptible	Select whether tasks assigned from another MRD can interrupt an agent. **Note** If you change the MRD from interruptible to non-interruptible or vice versa, the change takes effect once the agent logs out and then logs back in on that MRD.
Life	Enter the amount of time, in seconds, that the system waits before ending all tasks if the connection goes down.
Start Timeout	Enter the amount of time, in seconds, that the system waits for an agent to accept a task. When this time is reached, the system makes the agent Not Routable and re-queues the task.
Max Duration	Enter the maximum duration for a task, in seconds.
Max in Queue	Enter the maximum number of tasks allowed to be queued at one time.
Max Time in Queue	Enter the maximum amount of time, in seconds, a task can be queued.

Step 4 Click **Save**.

Dialed Number

Dialed numbers are string values used to select the appropriate routing script so that a voice call or a nonvoice task (such as an email or a request for a web chat) can be delivered to an agent. Each dialed number string is configured with a routing type and a Media Routing Domain and can be mapped to a call type. For incoming calls, you can configure post call survey and add the customized ringtone media file.

A typical call center requires multiple dialed number strings. In addition to creating dialed number strings for each telephone number that customers can use to reach you, you must set up dialed number strings for the following reasons:

- So that an agent can transfer to, or conference in, another agent
- For requery on no answer (RONA)
- For supervisor/emergency assist calls

Related Topics

Add and Maintain Dialed Numbers
Call Type, on page 192

Search for Dialed Numbers

The Search field in the Dialed Numbers 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:

- Enter a 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.)

Note Search by peripheral set is available only in Packaged CCE 4000 Agents and 12000 Agents deployments.

- Select departments, with options for **Globals and Departments**, **Globals only**, or **Departments only**.

  Selecting **Globals and Departments** or **Departments only** enables an input field where you can enter a space-separated list of department names. (Department is an OR search.)

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

Search by site is available only when remote sites are configured.

Add and Maintain Dialed Numbers

This procedure explains how to add a dialed number. For information on maintaining dialed numbers, see Update Objects and Delete Objects. After you have created Dialed Numbers, you can also add, or edit ringtone media files for multiple Dialed Numbers at once (see Add and Update Ringtone Media File for Multiple Dialed Numbers, on page 183).

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Dialed Number** tab.

Step 3 Click **New** to open the **New Dialed Number** window.

Step 4 Complete the following fields:

Field	Required?	Description
Dialed Number String	yes	The value used to route the call or direct the nonvoice task. Enter a string value that is unique for the routing type, maximum of 25 characters. **Note** The External Voice and PCS routing types must not have the same dialed number strings.
Description	no	Enter a maximum of 255 characters to describe the dialed number string.
Department	- (yes for departmental administrators)	A departmental administrator must select one department from the popup list to associate with this dialed number. The list shows all this administrator's departments. When a departmental administrator selects a department for the dialed number, the popup list for call type includes global call types and call types in the same department as the dialed number. A global administrator can leave this field as Global (the default), which sets the dialed number as global (belonging to no departments). A global administrator can also select a department for this Dialed Number. When an administrator changes the department, selections for call type are cleared if the selections don’t belong to the new department or the global department.
Site	-	The **Site** field displays Main by default for Packaged CCE 2000 Agents deployment. For Packaged CCE 4000 Agents and 12000 Agents deployments, **Site** is a mandatory field and has no default value. To add a site: **a.** Click the **magnifying glass** icon to display the list of sites. **b.** Select the required site.

Field	Required?	Description
Peripheral Set	Yes	This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see Add and Maintain Peripheral Set. To add a peripheral set: **a.** Click the **magnifying glass** icon to display the list of peripheral sets configured for the selected **Site**. **b.** Select the required peripheral set.

Field	Required?	Description
Routing Type	-	

Field	Required?	Description
		From the drop-down menu, select one of the following options: (For remote sites, options may vary depending on the PG types configured on the selected remote site.) • **External Voice:** Select this option for dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). These calls are referred to as external because they typically come from outside of the enterprise through a gateway. External Voice is the selection for calls that come in from customers and must be answered by agents or sent to the VRU. If you select External Voice, the **Ringtone Media File** field appears to enter the ringtone filename for the user-defined Dialed Numbers. For remote sites, the **External Voice** option is available if the site is configured to VRU PG. • **Internal Voice:** Select this option for dialed number strings that can be called from a Cisco Unified Communications Manager phone. These calls must have a route point on Unified Communications Manager that corresponds to the internally dialed number. They are referred to as internal because they can be accessed only by Unified Communications Manager. Internal Voice is used for dialed numbers that agents use to transfer calls to other agents, to enable the system to redirect calls internally when the agent doesn't answer, and to direct a call from an agent to a supervisor for assistance. Dialed numbers with the routing type Internal Voice appear on the Supervisor Script Dialed Number list when you create or edit a team. For remote sites, the **Internal Voice** option is available if the site is configured to Agent PG. • **Outbound Voice:** Select this option for dialed number strings that are used by the Cisco Outbound Option Dialer. These dialed number strings are referenced and used to route calls to agents or to VRU scripts in the Campaign Skill Group Selection. For remote sites, the **Outbound Voice** option is available if the site is configured to Multichannel PG. • **Post Call Survey:** Select this option for Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). This option is similar to External Voice where

Field	Required?	Description
		the calls come from outside of the enterprise through a gateway. However, Unified CVP directs the calls internally to Post Call Survey after agent ends the call. This option allows you to enter the Post Call Survey Dialed Number and associate the Dialed Number Patterns to the Post Call Survey Dialed Number. For remote sites, the **Post Call Survey** option is available if the site is configured to VRU PG. The following multichannel routing types are available if you have configured the peripherals for the multichannel machines using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory: • SocialMiner**:** Select this option for dialed number strings that originate from SocialMiner and are routed to an agent who interacts with a customer by Agent Request. • **Enterprise Chat and Email:** Select this option for dialed number strings that originate from Enterprise Chat and Email and are routed to an agent who interacts with a customer by email or by web chat. • **3rd Party Multichannel:** Select this option for dialed number strings that originate from a third-party application and are routed to an agent who interacts with a customer by email or by web chat. See the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html for information about configuring the peripherals using Peripheral Gateway Setup.
Media Routing Domain	no	The Media Routing Domain associated with the dialed number. Media Routing Domains (MRDs) organize how requests for media are routed. The system routes calls to agents who are associated with a particular communication medium; for example, voice or email. The selection of Routing Type determines what appears in this field. • If the Routing Type is External Voice, Internal Voice, or Outbound Voice, the Media Routing Domain is Cisco_Voice and you can't change it. • If the Routing Type is Multichannel, click the **magnifying glass** icon to display the **Select Media Routing Domain** popup window.

Field	Required?	Description
Call Type	no	Use the drop-down menu to select a valid call type to map to this dialed number strings. Associating a dialed number with a call type ensures appropriate routing and affects reporting. The default is the system default set in **Overview** > **Call Settings** > **Miscellaneous**. To select a different call type: • Click the **magnifying glass** icon to display the **Select Call Type** popup window. • Click a row to make a selection and close the list.
PCS Enabled Dialed Number Patterns	no	**Note** The **PCS Enabled Dialed Number Patterns** field appears if the **Routing Type** is **Post Call Survey**. Enter one or more dialed number patterns of type External Voice to transfer calls to the Post Call Survey dialed number entered in the **Dialed Number String** field. The field allows maximum of 512 characters that can have the comma-separated list without any spaces. Both alphanumeric and special characters are supported.
Ringtone Media File	no	**Note** The **Ringtone Media File** field appears if the **Routing Type** is **External Voice**. Enter filename of the custom ringtone for the user-defined Dialed Numbers - maximum of 256 characters without any spaces.

Step 5 Click **Save** to return to the List screen, where a message confirms the successful creation.

The configured Dialed Number is synchronized to Unified CVP machine deployed in Inventory. If the Sync fails, the Device Sync Alert icon appears on the status bar at the top-right of the List screen. Click the icon to perform the manual synchronization. See Device Out of Sync Alerts, on page 9

Add and Update Ringtone Media File for Multiple Dialed Numbers

You can add or edit a ringtone media file for multiple Dialed Numbers at once. The Dialed Numbers must be of the type **External Voice** to add or update the ringtone media filename.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Dialed Number** tab.
The List window appears with the configured dialed numbers.

Step 3 To add or update the ringtone media filename for multiple Dialed Numbers, check the check box that is associated with Dialed Numbers of the type **External Voice**.

Step 4 Click **Edit** > **Ringtone Media File**.
The **Edit Details of Dialed Number Strings** popup window appears.

Step 5 In **Ringtone Media File**, enter filename of the custom ringtone.

Step 6 Click **Save**, and then click **Yes** to confirm the changes.

Routing Pattern

A routing pattern comprises a string of digits (an address) and a set of associated digit manipulations that route calls to a destination which can be a device or a group of devices. Routing patterns provide flexibility in network design.

Search for Routing Patterns

The Search field on the Routing Pattern page offers an advanced and flexible search.

Click the + icon on the Search field to open a popup window, where you can:

- Enter a routing pattern, description, or destination to search for that string.
- Select a pattern type.
- Enter one or more site names separated by spaces. (Site is an OR search.)
- Select if Send to Originator is enabled.
- Select if RNA Timeout is configured.

Note Search by site is available only when remote sites are configured.

Add and Maintain Routing Pattern

This procedure explains how to add a routing pattern. For information on maintaining routing patterns, see Update Objects and Delete Objects.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Routing Pattern** tab.

Step 3 Click **New** to open the **New Routing Pattern** page.

Step 4 Complete the following fields:

Field	Required?	Description
Routing Pattern	yes	Enter a name for the routing pattern. Maximum length is 24 characters. Valid characters are alphanumeric, wildcard characters such as letter X, period (.), exclamation(!), greater than (>), and asterisk (*).

Field	Required?	Description
Description	no	Enter a description for the routing pattern. See Character Sets.
Site	-	Displays **Main** by default. Search and select the routing pattern site.
Pattern Type	yes	Select the type of pattern from the drop-down list.
Destination	yes	To select the SIP Server Group or FQDN: **a.** Click the field to open the **Add SIP Server Group** popup window. Based on the selected **Site** and **Pattern Type**, the popup window lists the SIP Server Groups. The SIP Server Groups are configured in **Call Settings** > **Route Settings** > **SIP Server Group**. **b.** Search and select a SIP Server Group from the list.
RNA Timeout	no	Enter the number of seconds that the destination should ring before the call is taken away. Range is 5 to 60 seconds.
Send to originator	no	Check the check box to configure calls to be sent to the originator. **Note** Send to originator is not applicable when you select the **VRU** pattern type for Cisco Virtualized Voice Browser (VVB).

Step 5 Click **Save**.

Location Configuration

The Location feature is used to route calls to the agent or IVR available in the local branch office instead of routing calls to the central or main office.

Locations are used to implement call admission control in a centralized call-processing system. In a centralized call-processing system, a single Cisco Unified Communications Manager cluster provides call processing for all locations on the IP telephony network. Call admission control enables you to regulate audio quality and video availability by limiting the amount of bandwidth that is available for audio and video calls over links between the locations.

If the required locations are configured in Cisco Unified Communications Manager (CUCM), Packaged CCE enable you to fetch the locations from CUCM through the Synchronization (Sync) option. This option allows you to select a Unified Communications Manager server and extract the location routing code. You can then assign the Ingress router to identify the call origin and subsequent routing.

Packaged CCE also allows you to create a new location and add location information.

Search for Locations

The Search field on the Location page offers an advanced and flexible search.

Click the + icon on the Search field to open a popup window, where you can:

- Enter name or description of a location to search for that string.
- Enter the hostname or IP address of the gateway. The search is case-insensitive and does not support partial matches.
- Enter a site. The search is case-insensitive and does not support partial matches.

Add and Maintain Location Configurations

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Location** tab.

Step 3 Click **New**.

Step 4 Complete the following fields:

Fields	Required?	Description
Location Name	Yes	Enter a name for the location.
Description	No	Enter a description of the location. See Character Sets.
Location Routing Code	Yes	A unique location code that is appended to the ICM label for routing the calls to the destination devices. See Location Properties, on page 187.
Sites	No Required if you add Gateways to the location.	Site of the location. The configured sites are listed in the **Sites** field. To add sites, select the applicable check boxes in the **Sites** field.
Gateways	No Required if you select Site(s) for the location.	Gateways that are associated with the location. To associate a gateway to the location: **a.** Click the + icon. The **Add Gateways** popup window opens with a list of gateways. **b.** Select a gateway from the list. Use the Search a List feature to navigate the list.

Step 5 Click **Save**.

Synchronize the Location Information

Location synchronization is a user-initiated task. A single synchronization operation runs in the background when initiated. When initiated, the system synchronizes and merges the locations from the Unified CM server selected during the configuration.

To complete a synchronizing operation:

- The system retrieves the location data from the Unified CM database.
- The system merges the retrieved data with any existing location data.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Location** tab.

Step 3 Click the **Sync** button.
The **Synchronize Location** popup window opens.

Step 4 Select a Unified CM server from the **Select CUCM Publisher** drop-down list.

Step 5 Click **Sync**.
The synchronized locations appear on the List window.

What to do next

You can add **Location Routing Code** and associate applicable **Sites** and **Gateways** to the required Locations.

Location Properties

The Location Properties feature provides options for the placement of the location routing code. The Location Properties setting applies to all the configured locations.

You can place the routing code at the beginning of the Network VRU label, in the middle of the Network VRU label and the correlation ID, or can choose not to insert the routing code.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Location** tab.

Step 3 Click the **Properties** link.
The **Properties** popup window opens.

Step 4 Select an option to insert the location routing code.

The options are:

- Insert routing code between Network VRU label and the correlation ID.
- Insert routing code at the beginning of the Network VRU label.
- Do not insert routing code.

The **Insert routing code between Network VRU label and the correlation ID** option is the default selection.

Step 5 Click **Save** to return to the List window.

What to do next

After you change the routing code insertion setting, you must recreate Routing Patterns and VVB Triggers associated to locations.

SIP Server Group

You can add the SIP Server groups to perform SIP dynamic routing by Cisco Unified Customer Voice Portal (CVP).

A SIP Server Group consists of one or more destination addresses (elements), and is identified by a Server Group domain name. This domain name is also known as the Fully Qualified Domain Name (FQDN).

Note The site specific SIP Server Groups' configuration is updated to all the Unified CVP of the corresponding site present in the Inventory (see System Inventory for Packaged CCE 2000 Agents Deployment).

Related Topics

Search for SIP Server Groups, on page 188
Add and Maintain SIP Server Group, on page 188
SIP Server Group Properties, on page 190

Search for SIP Server Groups

The Search field in the SIP Server Group tool offers an advanced and flexible search.

Click the + icon at the right of the Search field in the SIP Server Group tool. In the popup window, you can:

- Search for a name or description.
- Enter one or more site names separated by spaces (Site is an OR search).
- Select SIP Server type.
- Enter hostname/IP address of the element. The search is case-sensitive and does not support partial matches.

Note Search by site is available only when you configure remote sites.

Add and Maintain SIP Server Group

This procedure explains how to add a SIP Server Group. For information about maintaining SIP Server Groups, see Update Objects and Delete Objects.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **SIP Server Group** tab.

Step 3 Click **New** to open the **New SIP Server Group** page.

Step 4 Complete the following fields on the **General** tab:

Field	Required?	Description
Domain Name FQDN	yes	Enter the SIP Server Group Fully Qualified Domain Name (FQDN). Must be a valid FQDN limited to 128 characters. Can contain a combination of uppercase and lowercase alphanumeric characters, underscore [_], and period [.].
Description	no	Enter a maximum of 255 characters to describe the SIP Server Group. See Character Sets.
Site	-	To select the site of the group. Displays **Main** by default. To select a remote site: **a.** Click the magnifying glass icon to display the list of configured sites. **b.** Select the required site.
Type	yes	To select the type of group. From the drop-down list, choose one of the following options: • VRU - For Cisco Virtualized Voice Browser (VVB), Cisco Unified SIP Proxy (CUSP), and VXML Gateway devices. • Agent - For Cisco Unified Communications Manager (CUCM) and CUSP devices. • External - For Ingress Gateway and CUSP devices.

Step 5 Click **Members** tab.

a) Click the + icon.
The **Add Group Members** popup window appears with the hostname or IP address of the configured devices based on the **Site** and **Type** selected in the **General** tab.

Note To search a device configured in a different site, choose a site from the **Site** drop-down list.

b) Choose one or more devices from the **Add Group Members** popup window.
The selected devices appear in the **List of Group Members** table.

c) Enter appropriate values in the following fields:

Field	Required?	Description
Priority	yes	Priority of the element in relation to the other elements in the server group. Specifies whether the server is a primary or backup server. Primary servers are specified as 1. Range is 1 to 2147483647
Weight	yes	Weight of the element in relation to the other elements in the server group. Specifies the frequency with which requests are sent to servers in that priority group. Range is 10 to 2147483647.
Port	yes	Port number of the element in the server group. The default value is 5060. Range is 1 to 65535
Secure Port	no	The listening port for secure connection. Range is 1 to 65535

Step 6 Click **Save** to return to the List screen, where a message confirms the successful creation.

SIP Server Group Properties

The SIP Server Group properties configure the heartbeat parameters to exchange the heartbeat message between SIP Server Group elements and SIP Server Group.

Note The configuration of SIP Server Group properties forms the global setting for all SIP Server Groups across all sites.

Note The Up and Down Endpoint Heartbeat Interval is between any two heartbeats; however, it is not between heartbeats to the same endpoint. The SIP Server Group does not wake up at a specific interval and sends a heartbeat for all elements since this approach can result in CPU utilization issues. It also takes more resources to track heartbeats for many endpoints. For example, for 3 total elements across all SIP Server Groups, to proactively send a heartbeat to each element at 30000ms (30 seconds) intervals, you have to set the Endpoint Heartbeat Interval to 10000ms (10 seconds). It is less deterministic for reactive mode since elements that are currently down can fluctuate so the heartbeat interval fluctuates with it. To turn off pinging when the element is UP, set the UP interval to zero (reactive pinging). To turn off pinging when the element is down, set the DOWN interval to zero (proactive pinging). To ping when the element is either UP or DOWN, set both the intervals to greater than zero (adaptive pinging).

Update SIP Server Group Properties

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **SIP Server Group** tab.

Step 3 Click the **Properties** link.

The **SIP Server Properties** window opens to configure SIP Server Group properties.

Step 4 Update any of the following fields values:

Fields	Description	Default
Use Heartbeats to Endpoints	Check the check box to enable the heartbeat mechanism. Heartbeat properties are editable only when this option is enabled. **Note** Endpoints that are not in a Server Group can not use the heartbeat mechanism.	Enabled (Checked)
Number of Failed Heartbeats for Unreachable Status	The number of failed heartbeats before marking the destination as unreachable.	3
Heartbeat Timeout	The amount of time, in milliseconds, before timing out the heartbeat.	800 milliseconds
Up Endpoint Heartbeat Interval	The ping interval for heart beating an endpoint (status) that is up.	5000 millisecond
Down Endpoint Heartbeat Interval	The ping interval for heart beating an endpoint (status) that is down.	5000 millisecond
Heartbeat Local Listen Port	The heartbeat local socket listen port. Responses to heartbeats are sent to this port on CVP by endpoints.	5067
Heartbeat SIP Method	The heartbeat SIP method. **Note** PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.	OPTIONS
Heartbeat Transport Type	During transportation, Server Group heartbeats are performed with a UDP or TCP socket connection. If CVP Server encounters unreachable or overloaded callbacks invoked in the Server Group, that element is marked as being down for both UDP and TCP transports. When the element is up again, it is routable for both UDP and TCP. **Note** TLS transport is not supported.	UDP
Overloaded Response Codes	The response codes are used to mark an element as overloaded when received. If more than one code is present, it is presented as a comma delimited list. An OPTIONS message is sent to an element and if it receives any of those response codes, then this element is marked as overloaded.	503,480,600
Options Override Host	The contact header hostname to be used for a heartbeat request (SIP OPTIONS). The given value is added to the name of the contact header of a heartbeat message. Thus, a response to a heartbeat would contain gateway trunk utilization information.	cvp.cisco.com

Step 5 Click **Save**.

Call Type

Call types categorize calls. Based on call type, the system maps a dialed number to a routing script that ultimately sends the call to the appropriate destination. Consider the call types you need to create to meet your reporting needs, and configure a separate call type for each type of call treatment that you want to offer.

For example, you might create call types for the following:

- Calls answered by agents
- Calls abandoned at the VRU
- Calls that reroute when the agent does not answer
- Calls that are transferred and conferenced
- Outbound Option calls
- Calls that require supervisor assistance

Related Topics

Add and Maintain Call Types, on page 192
Dialed Number, on page 177

Add and Maintain Call Types

This procedure explains how to add a call type. For information on maintaining call types, see Update Objects and Delete Objects.

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings**.

Step 2 Click the **Call Type** tab.

Step 3 Click **New** to open the **New Call Type** window.

Step 4 Complete the following fields :

Field	Required?	Description
Name	yes	Enter a name for the call type using a maximum of 32 characters. This name must be unique among call types in the system.
Description	no	Enter a maximum of 255 characters to describe the call type. See Character Sets.

Field	Required?	Description
Service Level Threshold	no	This value is used in reports to identify the percentage of calls that are answered within that time threshold, enabling you to see whether agents are meeting the target goal. The field defaults to the System Default set in **Call Settings** > **Miscellaneous** > **Global** (see Global, on page 210). To select a different service level threshold, enter a value in seconds, from 0 to 2,147,483,647.
Service Level Type	no	Indicates how the system software calculates the service level. The field defaults to the System Default set in **Call Settings** > **Miscellaneous** > **Global** (see Global, on page 210). To override the system default for this call type, select one of these other options from the drop-down menu: • **Ignore Abandoned Calls:** Select this option to excludes abandoned calls from the service level calculation. • **Abandoned Calls have Negative Impact:** Select this option if you want only 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 time. • **Abandoned Calls have Positive Impact:** Select this option if you consider a call abandoned within the service level threshold time as a treated call. Abandoned calls have a positive impact on the service level.
Bucket Interval	-	Bucket intervals appear in call type reports and display the number of calls answered and abandoned for different time intervals. Configure the bucket interval associated with this call type. The field defaults to the System Default set in **Call Settings** > **Miscellaneous** > **Global** (see Global, on page 210). To select a different bucket interval: • Click the **magnifying glass** icon to display Select Bucket Interval. • Click the row to select a bucket interval and close the List.

Step 5 Click **Save** to return to the List window, where a message confirms the successful creation.

Expanded Call Variables

Calls can carry data with them as they move through the system. This data, called expanded call variable data, is embedded within the call and is visible to the agent on the agent desktop. ECC variables are passed back and forth in ECC payloads. Expanded call variable data can assist the agent in working with the caller.

The expanded call variable can be set or updated by Cisco Unified Customer Voice Portal (CVP), by Unified CCE scripting, or by an agent who is transferring the call.

- If the call is at Unified CVP for VRU treatment, the call context is exchanged between Unified CVP and Unified CCE.
- If the call is at an agent, the call context is exchanged between the desktop and Unified CCE.

Note that this is a two-way exchange: in some cases the expanded call variable data is sent to Unified CCE from Unified CVP or the agent desktop, and in some cases the data is sent by Unified CCE based on script configuration to Unified CVP or the agent desktop.

Built-in expanded call variables are identified by the **BuiltIn** check box on the Edit Expanded Call Variable window. You cannot delete these expanded call variables. You can create new expanded call variables subject to certain sizing constraints.

For Packaged CCE 4000 and 12000 Agents deployment, see *Configuration Guide for Cisco Unified Customer Voice Portal* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/products-installation-and-configuration-guides-list.html for the list of ECC Variables.

Related Topics

Add and Maintain Expanded Call Variables, on page 196
Sizing Expanded Call Variables, on page 199

ECC Payloads

You can define as many ECC variables as necessary. But, you can only pass 2000 bytes of ECC variables on a specific interface at any one time. To aid you in organizing ECC variables for specific purposes, the solution has *ECC payloads*.

An ECC payload is a defined set of ECC variables with a maximum size of 2000 bytes. You can create ECC payloads to suit the necessary information for a given operation. You can include a specific ECC variable in multiple ECC payloads.The particular ECC variables in a given ECC payload are called its *members*.

Note For ECC payloads to a CTI client, the size limit is 2000 bytes plus an extra 500 bytes for the ECC variable names. Unlike other interfaces, the CTI message includes ECC variable names.

In certain cases, mainly when using APIs, you might create an ECC payload that exceeds the CTI Server message size limit. If you use such an ECC payload in a client request, the CTI Server rejects the request. For an OPC message with such an ECC payload, the CTI Server sends the message without the ECC data. In this case, the following event is logged, “CTI Server was unable to forward ECC variables due to an overflow condition.”

You can use several ECC payloads in the same call flow, but only one ECC payload has scope at a given moment. TCDs and RCDs record the ID of the ECC payload that had scope during that leg of the call. The *Call.ECCPayloadID* variable contains the ID of the ECC payload which currently has scope.

In solutions that only use the default ECC payload, the system does not create an ECC variable that exceeds the 2000-byte limit for an ECC payload or the 2500-byte CTI Message Size limit.

Note Packaged CCE 2000 Agent deployment allows you to use only the default ECC payload for the Network VRU.

If you create another ECC payload, the system no longer checks the 2000-byte limit when creating ECC variables. The system creates the ECC variables without assigning them to an ECC payload. Assign the new ECC variable to an appropriate ECC payload yourself through the ECC Payload Tool.

You can create and modify ECC payloads in the **Configuration Manager** > **List Tools** > **Expanded Call Variable Payload List** tool. In Packaged CCE 4000 Agent and 12000 Agent deployments, you can assign an ECC payload to Network VRU using the Network VRU Explorer tool in Configuration Manager.

Default ECC Payload

The solution includes an ECC payload named "Default" for backward compatibility. If your solution does not require more ECC variable space, you only need the Default payload. The solution uses the Default payload unless you override it.

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

Note You cannot delete the Default payload. But, you can change its members.

Important During upgrades, when the system first migrates your existing ECC variables to the Default payload, it does not check the CTI message size limit. The member names might exceed the extra 500 bytes that is allocated for ECC payloads to a CTI client. Manually check the **CTI Message Size** counter in the **Expanded Call Variable Payload List** tool to ensure that the Default payload does not exceed the limit. If the Default payload exceeds the limit, modify it to meet the limit.

In a fresh install, the Default payload includes the predefined system ECC variables. In an upgrade, the Default payload's contents depend on whether the starting release supports ECC payloads:

- **ECC payloads not supported**—During the upgrade, a script adds your existing ECC variables to the Default payload.
- **ECC payloads are supported**—The upgrade brings forward the existing definition of your Default payload.

Note If your solution includes PGs from a previous release that does not support ECC payloads, the Router always sends the Default payload to those PGs. Those PGs can properly handle the Default payload.

ECC Payload Node

The **ECC Payload** node is available from the **General** tab on the **Object Palette**:

Figure 1: Payload icon

Use this node to change the ECC payload that has scope for the following part of your script. Once you select an ECC payload, it has scope for all non-VRU operations until changed. You can select the ECC payload either statically or dynamically by the payload's EnterpriseName or ID.

Add and Maintain Expanded Call Variables

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Route Settings** > **Expanded Call Variables** to open the **List of Expanded Call Variables**.

The window tracks the number of bytes used by the expanded call variables, measured against the system total and the CTI Server total.

Step 2 Click **New** to open the **New Expanded Call Variable** page.

Step 3 Complete the following fields:

Field	Required?	Description
Name	yes	The name of the expanded call variable, prepended by user. This field allows a maximum of 32 characters. (This maximum includes the four characters in user.)
Description	no	Enter up to 255 characters to describe the expanded call variable. There is no restriction of characters. See Character Sets.
Max Length	yes	Specifies the maximum number of characters allowed in the value that will be stored in the expanded call variable value. The range is from 1 to 210 characters.
Array	no	This check box is unchecked by default to indicate that the expanded call variable is scalar. Check the check box to configure the expanded call variable as an array, not a scalar.
Maximum Array Size	no	This field appears when Array is checked. Use it to indicate the maximum number of elements (1-255) in the array.

Field	Required?	Description
Enabled	no	Checking this check box indicates that the expanded call variable is currently enabled—it can be used in scripts and appears on the agent desktop.
Persistent	no	Checking this check box indicates that data for this expanded call variable will be written to the historical database; specifically to the Termination Call Detail (TCD) and Route Call Detail (RCD) tables. Note that storing excessive call variable data can degrade historical database performance. Only persistent call variables are written to the historical database. Nonpersistent variables can be used in routing scripts, but are not written to the database.
Cisco Provided	—	This check box is display-only, and appears when editing existing built-in or custom expanded call variables. The New Expanded Call Variable window does not include this check box.
Bytes Required (if enabled)	—	This display-only field indicates the number of bytes required to store the expanded call variable in the system.
Bytes Required in CTI Server (if enabled)	—	This display-only field is similar to Bytes Required, above, but applies to the CTI Server. In CTI Server, the number of bytes required includes the length of the expanded call variable name.
Total Bytes Required for Enabled Variables: # of maximum 2000 bytes (# bytes remaining)	—	This display-only field keeps a running total of the number of bytes used by all expanded call variables. The maximum limit allowed is 2000 bytes per ECC payload.
Total Bytes Required for Enabled Variables in CTI Server: # of maximum 2500 bytes (# bytes remaining)	—	This display-only field keeps a running total of the number of bytes used by all expanded call variables in CTI Server. The maximum limit allowed is 2000 bytes per ECC payload with an extra 500 bytes to add the names of the ECC variables in that payload.

Step 4 **Save** the expanded call variable and return to the List window, where a message confirms the successful creation.

What to do next

If you change the configuration of any ECC variable, 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.

Sizing Expanded Call Variables

Expanded call variable usage impacts PG, Router, and Logger bandwidth. The Expanded Call Variables List, Add, and Edit windows track the space that your expanded call variables are consuming, as compared with the system maximums.

The maximum amount of space that all the ECC variables in each ECC payload can take up in Unified Contact Center cannot exceed 2000 bytes.

Each expanded call variable in Unified CCE is calculated using the following formula:

- For scalar: 5 + Maximum_Length
- For array: 5 + (1 + Maximum_Length) * (Maximum_Array_Size)

The maximum amount of space that all the ECC variables in each ECC payload can take up in CTI Server cannot exceed 2500 bytes. The allowed limit is 2000 bytes per ECC payload with an extra 500 bytes to add the names of the ECC variables in that payload. Each expanded call variable in CTI Server is calculated using the following formula:

- For a scalar variable, the size is length of Name + Maximum Length + 4.
- For an array variable, the size is (length of Name + Maximum Length + 5) * Maximum Array Size.

IVR Settings

The IVR Settings page allows you to configure the Network VRU Scripts and File Transfers.

Network VRU Scripts

Not all calls are delivered directly to agents. Some are sent to a Voice Response Unit (VRU) instead of, or before, they are sent to an agent. In the Packaged CCE deployment, the VRU is Cisco Unified Customer Voice Portal (Unified CVP). You must configure network VRU scripts to direct Unified CVP on how to handle the treatment of individual calls, using Unified CVP microapplication functions.

There are six Unified CVP microapplication types:

- **Play Media (PM):** Retrieves and plays a media file such as a welcome.wav or an agent greeting.
- **Play Data (PD):** Retrieves and plays data of various types, such as numbers, characters, time of day, or currency.
- **Get Digits (GD):** Plays a media file and retrieves digits from the caller.
- **Menu (M):** Plays media menu file and retrieves a single telephone keypad entry from the caller.
- **Get Speech (GS):** A "GS,Server,V" script is provided with Packaged CCE and appears in the List of Network VRU Scripts.
- **Capture:** Allows you to trigger the storage of current call data at various points.

Related Topics

Access to VRU Scripts in Packaged CCE Routing Scripts

Add and Maintain Network VRU Scripts

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **IVR Settings** > **Network VRU Scripts** to open the **List of Network VRU Scripts**.

Step 2 Click **New** to open the **New Network VRU Script** window. Complete the following fields:

Field	Required?	Description
Name	yes	Enter a unique name to identify the script, using a maximum of 32 alphanumeric characters.
Description	no	Enter additional information about the script. See Character Sets.
Routing Type	yes	Retain the default (Voice) or select Multichannel from the drop-down menu. Voice routes the script to Unified CVP. Multichannel routes the script to Enterprise Chat and Email (ECE).
VRU Script Name	yes	Enter the name of the script as it is known on the Unified CVP. See VRU Script Name Parameters, on page 201.
Configuration Param	no	A string used by Unified CVP to pass additional parameters to the IVR Service. The content of the string depends on the microapplication to be accessed.
RNA Timeout	yes	Enter a number to indicate the number of seconds for the system to wait for a response from the routing client after directing it to run the script. The default value is 180 seconds. Valid values are 1 to 2147483647. The destination phone rings until it exceeds the ring-no-answer (RNA) timeout setting.
Interruptible	no	Checked by default, this check box indicates whether or not the script can be interrupted; for example, when an agent becomes available to handle the call.

Step 3 Click **Save** to return to the List window, where a message confirms the successful creation.

After you add a network VRU script, it is visible in the Script Editor Run External Script node. Processing this script node sends the network VRU script parameters to Unified CVP. After the system establishes that

the call has been successfully delivered, the Run VRU Script node executes, instructing Unified CVP to run the network VRU script and apply the call treatment.

Related Topics

VRU Script Name Parameters, on page 201
Sample VRU Script Names, on page 202
Configuration Parameters, on page 203
Sample Configuration Values, on page 206

VRU Script Name Parameters

VRU Script Name parameters have a “positional” sequence format-- the format is Micro_app acronym,parameter,parameter.

- The microapplication acronym is case-insensitive (enter PM or pm).
- Use double commas (,,) to skip a parameter; Unified CVP will supply the default.

The Play Media position sequence is PM,media file name,media library type,Uniqueness value.

The Play Data position sequence is PD,Data Playback Type,Uniqueness value.

The Get Digits position sequence is GD,media file name,media library type,Uniqueness value.

The Menu position sequence is M,media file name, media library type,Uniqueness value.

Parameter Name	Used For	Notes
Media File Name options are as follows: • A filename--(for instance, a .wav file) • (number 1-10)--Unified CVP plays the file in the corresponding Call.PeripheralVariable file. For example, a value of 2 instructs Unified CVP to look at Call.PeripheralVariable2. If you use the (number 1-10) option and set the Media Library Type to "V," Unified CVP plays the external VoiceXML file specified in the corresponding Call.PeripheralVariable. If you set the value to (no value) and set the Media Library Type to “A” or “S”, the IVR Service creates VoiceXML without a media prompt. • a--Unified CVP automatically generates the media file name for agent greeting when this option is specified. The filename is based on GED-125 parameters received from Unified ICM. This option is only valid if the Media Library Type is not set to V.	Play Media Get Digits Menu	**a** is used for PlayMedia only

Parameter Name	Used For	Notes
Data Playback Type options are as follows: • Number • Char (Character) • Date • Etime (Elapsed time) • TOD (Time of Day) • 24TOD (24-hour Time of Day) • DOW (Day of Week) • Currency (USD only)	Play Data	
Media Library Type Flag indicates the location of the media files to be played. Options are as follows: • A--(Default) Application • S--System • V--External VoiceXML	Play Media Get Digits Menu	**V** is an option for PlayMedia only.
Uniqueness value (optional) A string identifying a VRU Script Name as unique.	Play Media Play Data Get Digits Menu	

Sample VRU Script Names

This VRU Script Name	Instructs Unified CVP
PM,July,S	To use the Play Media (PM) microapplication to play the"July.wav" Media file, using the System (S) Media library.
PM,WebSite,,1	To use the Play Media (PM) microapplication to play the"Website.wav" media file, using the default Media Type (Application library), and setting 1 as the Uniqueness value.
GD,Password,A,O	To use the Get Digits microapplication to play the media file named password.wav, using the Application (A) media library and setting 0 as the Uniqueness value.
M,Main_Menu	To use the Menu microapplication to play the media file named Main_Menu.wav.

Configuration Parameters

Configuration parameters have a “positional” sequence format-- the format parameter,parameter,parameter.

Use double commas (,,) to skip a parameter; Unified CVP supplies the default.

The Play Media position sequence is *Barge-in allowed,RTSP Timeout,Type-ahead Buffer Flush*.

The Play Data position sequence is *Location of files to be played,Barge-in allowed,Time Format,Type-ahead Buffer Flush*.

The Get Digits position sequence is *Minimum Field Length,Minimum Field Length,Barge-in allowed,Inter-digit Timeout,No Entry Timeout,Number of Invalid Tries,Timeout Message Override,Invalid Entry Message Override,Dtmf Termination Key,IncompleteTimeout*.

The Menu position sequence is *List of Menu Choices,Barge-in allowed,No Entry Timeout,Number of No Entry Tries,Number of Invalid Tries,Timeout Message Override,Invalid Entry Message Override*.

Parameter Name	Used For	Notes
Barge-in Allowed Valid options are as follows: • Y--Barge-in is allowed. Note that DTMF barge-in is supported. Voice barge-in is not. • N --(Default) Barge-in is not allowed	Play Media Play Data Get Digits Menu	Unified CVP handles barge-in as follows: • If barge-in is not allowed, the SIP/H.323 Service/Gateway continues prompt play when a caller starts entering digits, and the entered digits are discarded. • If barge-in is allowed, the H.323Service/Gateway discontinues prompt play when the caller starts entering digits.
DTMF Termination Key A single character that, when entered by the caller, indicates digit entry is complete. Valid options are as follows: • 0 to 9 • * (asterisk) • # (pound sign, the default) • N (no termination key)	Get Digits	
Incomplete Timeout The amount of time after a caller stops speaking to generate an invalid entry error because the caller input does not match the defined grammar. The valid options are 0 to 99. The default is 3.	Get Digits	V is an option for Play Media only.

Parameter Name	Used For	Notes
Inter-digit Timeout The number of seconds the caller is allowed between entering digits. If exceeded, the system times out. The valid options are 1 to 99. The default is 3.	Get Digits	
Invalid Entry Message Override The valid options are: • Y--Override the system default with a pre-recorded Application Media Library file • N-- (Default) Do not override the system default	Get Digits Menu	
List of Menu Choices Valid options are as follows: • 0 to 9 • * (asterisk) • # (pound sign)	Menu	Formats allowed are: • Individual options delimited by a / (forward slash) • Ranges delimited by a - (hyphen) with no space
Location of the data to be played Valid options are as follows: • Null--(Default) If you leave this option empty, the system uses the expanded call variable named user.microapp.play_data. • A number representing a Call Peripheral Variable number (for example, a 1 to represent Call.PeripheralVariable1).	Play Data	
Maximum Field Length Maximum number of digits entered by the caller. The valid options are 1 to 32. The default is 1.	Get Digits	
Minimum Field Length Minimum number of digits entered by the caller. The valid options are 1 to 32. The default is 1.	Get Digits	
No Entry Timeout The number of seconds a caller is allowed to begin entering digits. If exceeded, the system times out. The valid options are 0 to 99. The default is 5.	Get Digits Menu	
Number of Invalid Tries Unified CVP repeats the "Get digits" cycle when the caller enters invalid data. (Total includes the first cycle.) The valid options are 1 to 9. The default is 3.	Get Digits Menu	

Parameter Name	Used For	Notes
Number of No Entry Tries Unified CVP repeats the "Get Digits" cycle when the caller does not enter any data after the prompt has been played. (Total includes the first cycle.) The valid options are 1 to 9. (The default is 3.)	Get Digits Menu	
RTSP Timeout Specifies the Real-time Streaming Protocol (RTSP) timeout—in seconds—when RTSP is used. The valid range is 0 to 43200 seconds. The default is 10 seconds. If the value is set to 0 or a timeout value is not provided, the stream will not end.	Play Media	
Time format Valid only for the time Data Playback types Etime, TOD, and 24TOD. The available formats are as follows: • Null--Leave this option empty for non-time formats • HHMM--Default for time formats • HHMMSS • HHMMAP--Includes a.m. or p.m.; valid only for TOD	Play Data	
Timeout Message Override. The valid options are as follows: • Y--Override the system default with a pre-recorded Application Media Library file • N--(Default) Do not override the system default	Get Digits Menu	

Parameter Name	Used For	Notes
Type-ahead buffer flush The Cisco VoiceXML implementation includes a type-ahead buffer that holds DTMF digits collected from the caller. When the VoiceXML form-interpretation algorithm collects user DTMF input, it uses the digits from this buffer before waiting for further input. This parameter controls whether the type-ahead buffer is flushed after the prompt plays out. A False value (default) means that the type-ahead buffer is not flushed after the prompt plays out. If the prompt allows barge-in, the digit that barges in is not flushed. Valid options are as follows: • Y—Flush the type-ahead buffer • N—(Default) Do not flush the type-ahead buffer	Play Media Play Data	

Sample Configuration Values

This Configuration sequence	Instructs Unified CVP
(for a Menu microapplication) 0-2/9,,4,2,2	To accept numbers 0, 1, 2, and 9. , (Skipped parameter) To accept the default barge-insetting (Y). To set the no entry timeout value to 4 seconds. To allow 2 no entry tries. To allow 2 invalid tries. To accept all other defaults.
(for a Get Digits microapplication) GD,Password,A,O	To use the Get Digits micro-application to play the media file named password.wav, using the Application (A) media library and setting 0 as the Uniqueness value.
(for a Menu microapplication) M,Main_Menu	To use the Menu micro-application to play the media file named Main-Menu.wav.

File Transfers

Use the **File Transfers** page to transfer the VXML application files to VXML Servers. Upload the application files to the Administration and Data Server (AW) and deploy the application files on the VXML Server.

Click the file transfer record to view the details for that file transfer. On the details page, you can also download the job details file and the log file for a file transfer job.

Add Files to Server

This procedure explains how to upload files to the AW.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **IVR Settings** > **File Transfers**.

Step 2 Click **New** to open the **New File Transfer** page.

Step 3 Click **Add to Server** to open the **Upload File** pop-up.

Note You can upload one file at a time.

Step 4 Click **Click to select** and select a zip file to upload.

Step 5 Click **Upload**.

The file is uploaded to AW and listed under **Available Files in the Server**.

Note You can hover over a row and click the **x** icon to delete a file from the server.

Add and Maintain File Transfers

This procedure explains how to create a new file transfer job. For information on deleting file transfers, see Delete Objects, on page 7.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Call Settings** > **IVR Settings** > **File Transfers**.

Step 2 Click **New** to open the **New File Transfer** page.

Step 3 Select one or more sites for the file transfer.

Step 4 Enter a description for the file transfer.

Step 5 On the **Available Files in the Server** list, select the files that you want to transfer and click **Save**.
This initiates the transfer of the selected files to VXML Server of the selected sites.

View Details for a File Transfer

On the **IVR Settings** page > **File Transfers** tab, click the file transfer record to view the details for that file transfer.

For details page fields' description, refer the following table:

Field	Description
State	Shows one of the following status options for the file transfer: • **Queued:** Indicates that the file transfer job has been queued and is processed after any file transfer jobs submitted ahead of it are completed. When multiple file transfer jobs are submitted, they are run in the order they are created. • **Processing:** Indicates that the file transfer is being processed. • **Succeeded:** Indicates that all operations in the file transfer were successful. • **Partially Succeeded:** Indicates that some operations were successful, and some were unsuccessful. • **Failed:** Indicates that all operations were unsuccessful. • **Cancelled**: Indicates that the file transfer job is cancelled when the preceding job is terminated due to unrecoverable error while this job was in the queued state.
Description	Displays the description of the file transfer.
Host	Displays hostname of the Administration and Data server where the file transfer was initiated and is stored.
Creation Time	Displays the date and time the file transfer was submitted.
Start Time	Displays the date and time the file transfer entered the processing state.
Total Time	Displays the total time taken for processing the file transfer to reach the current state.
Job Details	Click the download icon to open or download the file transfer job details file in .csv format.
Log File	Click the download icon to open or download the log file (in .txt format) for this file transfer job. If the job is in processing state, click the download icon to view the job progress. A log file is generated for each file transfer job. The log file contains detail of each operation that was run, and a summary indicating if the file transfer is completed successfully or had failures.

Bucket Intervals

Configure bucket intervals to report on how many calls are handled or abandoned during specific, incremental time slots. Each bucket interval has a maximum of nine configurable time slots, called *Upper Bounds*. Upper Bounds are ranges measured in seconds to segment and capture call-handling activity. You can run reports that show calls answered and calls abandoned for these intervals.

For example, if your goal is to have calls handled within 1 minute, you might set up Upper Bounds for intervals that show how many calls are handled in less than or more than 1 minute. Intervals might be for 30 seconds, 60 seconds, 80 seconds, 120 seconds, 150 seconds, 180 seconds, and 240 seconds. Using these intervals, you can see if calls are being answered within 1 minute or if callers are waiting longer. The intervals also give you insight into how long callers are willing to wait before abandoning a call. Perhaps many callers do not abandon a call until they have waited for two minutes. This might indicate that you can modify your goal.

You can associate bucket intervals with call types, skill groups, and precision queues.

The system automatically creates a built-in bucket interval, which you cannot edit or delete.

Add and Maintain Bucket Intervals

Procedure

Step 1 In **Unified CCE Administration**, navigate to **Overview** > **Call Settings** > **Bucket Intervals**.

Step 2 Click **New** to open the **New Bucket Interval** window.

Step 3 Complete the following fields:

Field	Required?	Description
Name	yes	Enter a name for the call type using a maximum of 32 characters.
Upper Bound 1	yes	Enter a value in the Upper Bound 1 field, using a number greater than 0 and less than 2147483647. This value is interpreted as seconds. For example, your entry of 10 in this field creates an Upper Bound 1 interval with a time slot of 0 to 10 seconds.
Upper Bound 2 - 9	no	The value for each Upper Bound must be higher than the value of the previous Upper Bound. If you leave an Upper Bound field blank, all remaining fields must be blank. For example: To configure three intervals that span 10 seconds each and then have all other calls grouped into an interval that extends beyond your third defined interval, enter the following values: • Upper Bound 1 interval: 10 This time slot is 0 to 10 seconds. Reports will show the total number of calls answered and calls abandoned from 0 to 10 seconds. • Upper Bound 2 interval: 20 This time slot is any time greater than 10 seconds and less than 20 seconds. Reports will show the total number of calls answered and calls abandoned between 10 and 20 seconds. • Upper Bound 3 interval: 30 This time slot is any time greater than 20 seconds and less than 30 seconds. Reports will show the total number of calls answered and calls abandoned between 20 and 30 seconds. • All other Upper Bound fields blank. Reports will show the total number of calls answered and calls abandoned after 30 seconds.

Step 4 Click **Save** to return to the List screen, where a message confirms the successful creation of the bucket interval.

Miscellaneous

Use this page to configure miscellaneous call settings. The **Unified CCE Administration** > **Call Settings** > **Miscellaneous** page has various tabs such as Global, Main Site, and the configured remote sites. Navigate to the required tab to configure the settings.

Note Packaged CCE 4000 Agents and 12000 Agents deployment contains the Global tab only.

Global

This tab contains the following sections:

- Congestion Control
- Agent
- Call Reporting
- Script

Congestion Control

You can review congestion control fields in this section. This section contains the following fields:

Field	Description
Congestion Control fields	• **Treatment Mode** This display-only field shows Treat call with DN default label. • **System Default Label** This display-only field is blank for Packaged CCE and Packaged CCE Lab Mode deployments. If your system was changed from another deployment type, this field retains the system default label for that deployment. • **Maximum Calls Per Second** This display-only field displays the current value for maximum calls per second for the deployment.

Agent

Enter values in this section to define system-level values for agents. This section contains the following fields:

Field	Required?	Description
Minimum Password Length	yes	Enter a value between 0 and 32 to set the minimum required length for passwords. Changing this value affects new passwords only and does not apply to existing ones.
Username Case Sensitivity	no	Check this check box to indicate that all usernames are case-sensitive. Leave it unchecked to indicate that case does not matter.

Call Reporting

Enter values in this section to define system-level values for calls. This section contains the following fields:

Field	Required?	Description
Bucket Interval	yes	Click the **magnifying glass** icon to display the popup list of configured bucket intervals. Select a bucket interval to use as the system default. You can change the bucket interval for individual call types, skill groups, and precision queues. (See Call Type, on page 192, Skill Groups, on page 106, and Precision Queues, on page 111.)
Call Type	yes	Click the **magnifying glass** icon to display the popup list of configured call types. Select a call type to use as the system default. You can change the call type for individual Dialed Number, on page 177.
Service Level Type	yes	From the drop-down menu, select an option to configure the default method by which the system software calculates the service level type. You can change the service level type for individual call types and precision queues. You have the following service level options: • **Ignore Abandoned Calls:** This selection excludes abandoned calls from the service level calculation. • **Abandoned Calls have Negative Impact:** Select this if you want only 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 time. • **Abandoned Calls have Positive Impact:** Select this if you consider a call abandoned within the service level threshold time as a treated call. Abandoned calls have a positive impact on the service level.
Service Level Threshold	yes	Enter a value in seconds, from 0 to 2,147,483,647, for the maximum time that a caller spends in a queue before being connected to an agent. This value is used in reports to identify the percentage of calls that are answered within that time threshold, enabling you to see whether agents are meeting the target goal. Set the value to 0 seconds if you do not want a service level threshold to be set for calls. The value here sets the system default for service level threshold. You can change the value for individual call types and precision queues. (See Call Type, on page 192 and Precision Queues, on page 111.)
Abandon Call Wait Time	yes	Enter a value in seconds (between 1 and 14400) to configure the minimum time an incoming call must be queued before the call is considered abandoned if the caller disconnects the call.
Answered Short Call Threshold	no	Enter a value in seconds (between 0 and 14400) to configure the maximum duration for a short call. Calls with a duration below that value are considered short. Set the threshold to factor out short calls from handle times.

Field	Required?	Description
Reporting Interval	yes	From the drop-down menu, select **15 Minutes** or **30 Minutes** to configure the system to store historical information in 15-minute or half-hour summaries. The Unified CCE PG sends these records to the Logger, which in turn writes them to the Central Database. Note that the 15-minute interval requires a larger amount of database space than the 30-minute interval.

Script

Use this section to set the number of retained script versions.

Field	Description
Script Versions to Retain	Enter a value from 1 to 100 to define the maximum number of versions of each routing script you want to maintain in the database. When you select a number, the system automatically deletes the oldest version when the limit is exceeded.

Login Session

Main Site

This tab contains the following sections:

- Agent
- Labels

Agent

Enter values in this section to define system-level values for agents. This section contains the following fields:

Field	Required?	Description
Desk Settings	yes	Click the **magnifying glass** icon to display the popup list of configured desk settings. This list shows only global desk settings. The desk settings you select will be the system default for all agents. You can change the desk settings for individual agents. (See Add and Maintain Agents, on page 80.)
Agent Phone Line Control	yes	Select Single Line or All Lines to indicate whether all agents supported on the agent peripheral can have one or more than one line configured. **Important** • If you select All Lines, you must access Cisco Unified Communications Manager to set Busy Trigger to 1 and Max Number of Calls to 2 for each phone. Use the Unified Communications Manager Bulk Administration tool to change these settings for all agent devices. • If you change the Agent Phone Line Control setting, you must restart the peripheral gateways for the change to take effect. To restart the PGs, access the Unified CCE PG on Side A and Side B. Open Service Control and restart all PG services on Side A and Side B.

Labels

Use this section to view and edit labels for Unified CM, Outbound, and Unified CVP. This section contains the following fields:

Field	Description
Unified CM Label	This field contains a 10 digit string that matches the Unified CM route pattern.
Outbound Label	This field contains a 10 digit string that matches the IOS Voice Gateway dial-peer.
Unified CVP Label	This field contains a 10 digit string that matches the CVP dialed number pattern. When this label is used for all Unified CVP routing clients, the **Same Label for All Unified CVPs** check box is checked. To use a different label for each Unified CVP routing client, uncheck the **Same Label for All Unified CVPs** check box, and enter a 10 digit string in each routing client field.

Remote Sites

The miscellaneous settings vary based on the type of peripheral gateways configured for a particular remote site.

PGs Configured	Settings
Agent	Agents, Unified CM Label
VRU	Unified CVP Label
Multichannel	Outbound Label

If a remote site has all the PGs configured, the settings options are same as that of Main Site. If it has a combination of two PGs configured, the respective combination of settings appears.

Feature Setup

Manage Features

Packaged CCE webadmin provides the following optional features that you can configure anytime after your Packaged CCE system is installed, configured, and operational:

Courtesy Callback

To improve caller and workforce experience, Packaged CCE enables you to configure Courtesy Callback feature. The Courtesy Callback feature is available in Unified CVP.

With Courtesy Callback, the caller can choose to receive a callback from the contact center, rather than having to wait for an extended time on hold. Callers do not lose their place in the queue. The feature allows the system to offer callers who meet certain criteria, for example, callers with the possibility of being in the queue for more than X minutes, the option to be called back by the system when the wait time would be considerably shorter.

The system collects callback information from the caller, monitors the agent availability, and calls the customer when the agent is close to available. For example, if the caller decides to be called back by the system, then they leave their name and phone number. When the system determines that an agent is available (or will be available soon), then a call is placed back to the caller. The caller must answer the call and indicate that they are the caller. The caller is connected to the agent after a short wait.

To set up Courtesy Callback, you must configure Ingress Gateway, VXML Gateway, Call Studio, and CCE Scripts. For more information on the Courtesy Callback feature, see *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Configure Courtesy Callback

Before you begin

A CVP Reporting Server is required for the Courtesy Callback feature. The Reporting Server must be installed before completing the following task. Download the self-signed certificate for CVP Reporting Server from the browser, and import the certificate to the AW machine. For instructions to install the CVP Reporting server and import the self-signed certificate to AW machine, see the *Cisco Packaged Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Features** > **Courtesy Callback**.

Step 2 From the **Site** drop-down list, choose a site for which you want to configure the Courtesy Callback feature. By default, it is 'Main'.

Step 3 From the **CVP Reporting Server** drop-down list, choose a Reporting Server to use for storing Courtesy Callback data.

Note The list includes all the Reporting Servers configured for the site.

If you leave the selection blank by selecting '-', no Reporting Server is associated with the Courtesy Callback deployment.

Step 4 In the **Dialed Number Configuration** section, complete the following:

Fields	Required?	Description
Maximum Callbacks per Dialed Number	Yes	By default, the **Unlimited** option is selected, which is equivalent an unlimited number of callbacks offered per calling number. Th maximum value is 1000. To limit the number of calls, from the same calling number that a eligible to receive a callback: **a.** Select the **Limited** option. **b.** Enter a positive number in the text field to allow Courtesy Callback to validate and allow the specified number of callba per calling number.
Allow unmatched Dialed Numbers	No	Check the **Allow unmatched Dialed Numbers** check box to allo callbacks to the dialed numbers that are not available in the **Allow Dialed Number Patterns** list. **Note** If no dialed numbers are present in the **Allowed Dial Number Patterns** list, then Courtesy Callback does n allow any callbacks.
Allowed Dialed Number Patterns	No	The list of allowed dialed numbers to which callbacks can be sen By default, the list includes preconfigured allowed dialed numbe patterns. To add a dialed number pattern: **a.** Click the '+' icon and enter a dialed number pattern. Valid characters are alphanumeric, period (.), Exclamation (! asterisk(*), greater than(>), and backslash (\). The field does allow you to enter any invalid characters. **b.** Click **Add**. To remove a dialed number pattern, click the 'x' icon associated w the number in the list.

Fields	Required?	Description
Denied Dialed Number Patterns	No	The list of denied dialed numbers to which callbacks are never sent. By default, the list includes preconfigured denied dialed number patterns. To add a dialed number pattern: **a.** Click the '+' icon and enter a dialed number pattern. Valid characters are alphanumeric, period (.), Exclamation (!), asterisk(*), greater than(>), and backslash (\). The field does not allow you to enter any invalid characters. **b.** Click **Add**. To remove a dialed number pattern, click the 'x' icon associated with the number in the list. Denied numbers take precedence over allowed numbers. • Wildcarded DN patterns can contain "." and "X" in any position to match a single wildcard character. • Any of the wildcard characters in the set ">*!" matches multiple characters but can only be used trailing values because they always match all remaining characters in the string. • The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match. • When the number of characters match equally by wildcarded patterns in both the Allowed Dialed Numbers and Denied Dialed Numbers lists, precedence is given to the one in the Denied Dialed Numbers list.

Step 5 Click **Save**.

Context Service

Cisco Context Service is a cloud-based omnichannel solution for Cisco Contact Center Enterprise Solutions. It enables you to capture your customer's interaction history by providing flexible storage of customer-interaction data across any channel.

Various components in the CCE Solution provide out of the box integration with Context Service. Context Service also provides an API for integration with your own applications or third-party applications to capture end-to-end customer-interaction data.

For more information about Context Service, see *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html

Register Cisco Customer Voice Portal (CVP), Cisco Finesse, SocialMiner and Enterprise Chat and Email with Context Service

From the Unified CCE Administration Context Service tool, you can register CVP, Finesse, SocialMiner and Enterprise Chat and Email with Context Service in order to store data about tasks from these applications. For SocialMiner, Context Service can store data about tasks from the Task Routing APIs.

Note If you are in a non-Packaged CCE deployment, or Packaged CCE 4000 Agents and 12000 Agents deployments, use the System Inventory to set the Principal AW to manage credentials for Context Service before registering.

When registering with Context Service:

- For Packaged CCE deployments, the Unified CCE AW must be able to reach Context Service.
- For non-Packaged CCE deployments, or Packaged CCE 4000 Agents and 12000 Agents deployments, the Principal AW that manages Context Service credentials must be able to reach Context Service.
- You are asked to provide administrator credentials for your organization.

In addition to registering:

- Add SocialMiner to the System Inventory in order to connect with Context Service.
- Enable the built-in POD.ID expanded call variable to send task context data through the system.

  For Packaged CCE, use the Expanded Call Variable tool in Unified CCE Administration. For other deployments, use the Expanded Call Variable List tool in Configuration Manager.

Deregister CVP, Finesse, SocialMiner from Context Service

If you no longer want to use Context Service with CVP, Finesse, SocialMiner and Enterprise Chat and Email, you can deregister. You are asked to provide the administrator credentials that you used to register to Context Service.

Configure Context Service Settings

Use the Context Service tool in Unified CCE Administration to register Unified CVP, Finesse, SocialMiner and Enterprise Chat and Email to the Context Service.

For more information about Context Service registration, see https://cisco.com/go/contextservice.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Features** > **Context Service**.

Step 2 Complete the following parameters and click **Save**.

Field	Description
Proxy Server URL	Optional. If you are using a proxy server to connect to Context Service, enter the URL of the proxy server.

Field	Description
Timeout	The amount of time, in milliseconds, that the system waits for a response from Context Service before abandoning the attempt to perform the operation. Valid values are 200 to 15000 ms. Default is 1200 ms.
Lab Mode	Whether Context Service is in lab mode. Default is false (unchecked).

Step 3 To register with Context Service, click **Register**.

Step 4 After a successful registration, you can deregister from the Context Service by clicking **De-Register**.

What to do next

If you configured a proxy server for Context Service, configure the browser proxy with the proxy server URL you specified. Refer to your browser's documentation for information about configuring proxy settings.

Related Topics

System Inventory for Packaged CCE Deployments

Set up Single Sign-On

Before you begin

- Disable pop-up blockers. This is necessary to see all test results correctly.
- If you are using Internet Explorer, verify that it is not in Compatibility Mode and that you are using the AW's fully qualified domain name to access CCE Administration (for example, **https://fully-qualified-name.com/cceadmin**).

Procedure

Step 1 In **Unified CCE Administration**, choose **Features** > **Single Sign-On**.

Step 2 On the **Single Sign-On (SSO)** page, click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error, and then click **Retry**.

Step 3 When registration has completed successfully, click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when prompted, log in as a user that has SSO credentials.

The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click Test again.

Test results are not saved. If you refresh the page, run the test again before enabling SSO.

Step 4 Select the SSO mode for the system from the **Set Mode** drop-down list:

- Non-SSO: This mode disables SSO for all agents and supervisors. They use existing Active Directory-based and local authentication.
- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically. If you have already set the SSO mode for the system, the SSO mode is set on those machines automatically.

Third-party Integration

Note To enable this feature in Packaged CCE 12.0(1), install the ICM12.0(1)_ES patch. For more information, see *Release Notes for Packaged Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-release-notes-list.html.

Note Third-party gadgets can be added or modified only from a principal AW machine.

Third-party integration enables you to add user interfaces of third-party components your Contact Center employs in to Unified CCE Administration. You can add custom gadgets such as an agent reskilling gadget or third-party pages such as a browser-based CRM tool. Integrate the user-interfaces and administer multiple third-party components from Unified CCE Administration.

This feature also allows you to personalize the layout of Unified CCE Administration.

The system-defined cards in the layout have been placed in the order in which an administrator would typically use them. Menus with common or similar functionalities are grouped in a single card or menu. (For example, the User Setup card contains menus that allow you to manage agents, administrators, and assign permissions to user roles.)

You can add the third-party user interface to system-defined menu or card with a common or similar functionality. If the functionality does not match, add the third-party user interface to a user-defined menu or card. For more information on how to customize the layout, see Customize the Unified CCE Administration Layout, on page 224.

Role-Based Access

Only system administrators can add, edit, or delete a third-party user interface and customize the Unified CCE Administration layout.

System administrators can assign access to a third-party user interface to custom roles. For information on how to assign access, see Assign Access to Administrators, on page 222

Manage Third-party Integration

Complete the following procedures to add, edit, search, and delete the third-party user interfaces.

Add Third-party User Interface

While adding a third-party user interface, you can define data that the third-party user interface can use while its rendered. Define the data as custom key-value pairs or choose from an array of system-defined data.

For example, define a custom key-value pair called "license-key" with a fixed value, which a third-party page can use to call an API from its own server. Select system-defined data such as "Current User" so that the user interface can call UnifiedConfig API.

Note You can access a UnifiedConfig API from the third-party user inteface only if the role you are assigned with has the required permissions. For more information on Packaged CCE APIs and how to use them, see the *Cisco Packaged Contact Center Enterprise Developer Reference Guide*.

Complete the following procedure to add a third-party user interface to Unified CCE Administration.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Features** > **Third-party Integration**.

Step 2 On the **Manage Third-party Integration** tab, click **New**.

Step 3 In the **General Tab** complete the following.

Field	Description
General Tab	
Integrate as Gadget	Select this check box if you are adding a custom gadget. Leave the check box unselected, if you are adding a third-party page.
URL	Enter the secure URL of the third-party user interface.
Name	Enter a unique name for the third-party user interface, using a maximum of 15 characters. There is no restriction on the special characters. **Note** Once the third-party user interface is added, you cannot change the name.
Description	Optional. Enter up to 255 characters to describe the third-party user interface. There is no restriction on the special characters.

Field	Description
System Defined Data	Optional. Define data that the third-party user interface can use while its rendered. Click + and select from the following list. • **Deployment Type**: The current deployment type. • **Current User**: The credentials of the logged on user. • **Current Role**: The role of the logged on user. • **API-based URL**: The base URL on to which the APIs are loaded. • **Locale**: The current locale setting.
User Defined Data	Optional. Define custom key-value pairs you need to render the third-party user interface. To add a key-value pair: **a.** Click +. **b.** Enter the name and value in the respective fields. **Note** The **Value** field is optional. You can only enter up to 1024 characters in the **Value** field. **c.** Optional. Hide the value you enter by selecting the **Mask** check box. **d.** Click ✓ to add. **e.** To add another parameter, click + again.

Step 4 To set the placement of the third-party user interface in the Unified CCE Administration layout, click the **Placement** tab.

To add to a new menu in a new card:

a) Scroll using the < and > icons and select the **Add New Card** card.
b) Click ✎ to choose a color and icon for the card.
c) Click ✎ next to **Add Title** to enter the card title.
d) Click **Save**. The new card is displayed in the list of cards.
e) In the new card, click ✎ to enter the menu name. Click ✓ to save.

Note You can only add up to eight cards.

To add to a new menu in a system-defined card:

a) Scroll using the < and > icons to select a system-defined card.
b) Click ✎ to enter the menu name. Click ✓ to save.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

To add to a system-defined menu in a system-defined card:

a) Select the menu by clicking on it. The selected menu is highlighted in a red box.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

Step 5 Click **Save**.

What to do next

Assign Access to Administrators, on page 222

Assign Access to Administrators

System administrators can assign access to the third-party user interface to custom roles. Complete the following procedure to assign access.

Procedure

Step 1 Go to **User Setup** > **Roles**.

Step 2 Select the custom role.

Step 3 Under **Third-party Integration**, select the check box that is named after the third-party user interface (for example, if the name of the third-party user interface is "CRM", **CCE Administration** creates a checkbox named "CRM") and click **Save**.

Access to the third-party user interface is assigned to the custom role.

Edit Third-party User Interface

Complete the following procedure to edit a third-party user interface.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Features** > **Third-party Integration**.

Step 2 From the list of pages, click the row of the page or gadget you want to edit.

Step 3 Edit the following fields.

Field	Description
General Tab	
Integrate as Gadget	Select this check box if you are adding a custom gadget. Leave the check box unselected, if you are adding a third-party page.
URL	Enter the secure URL of the third-party user interface.
Name	This field is not editable.
Description	Optional. Enter up to 255 characters to describe the third-party user interface. There is no restriction on the special characters.

Field	Description
System Defined Data	Optional. Define data that the third-party user interface can use while its rendered. Click + and select from the following list. • **Deployment Type**: The current deployment type. • **Current User**: The credentials of the logged on user. • **Current Role**: The role of the logged on user. • **API-based URL**: The base URL on to which the APIs are loaded. • **Locale**: The current locale setting. For more information, see the *Cisco Packaged Contact Center Enterprise Developer Reference Guide*
User Defined Data	Optional. Define custom key-value pairs you need to render the third-party user interface. To add a key-value pair: **a.** Click +. **b.** Enter the name and value in the respective fields. **Note** The **Value** field is optional. You can only enter up to 1024 characters in the **Value** field. **c.** Optional. Hide the value you enter by selecting the **Mask** check box. **d.** Click ✓ to add. **e.** To add another parameter, click + again.

Step 4 To change the placement of the third-party user interface in the Unified CCE Administration layout, click the **Placement** tab.

To add to a new menu in a new card:

a) Scroll using the < and > icons and select the **Add New Card** card.
b) Click ✎ to choose a color and icon for the card.
c) Click ✎ next to **Add Title** to enter the card title.
d) Click **Save**. The new card is displayed in the list of cards.
e) In the new card, click ✎ to enter the menu name. Click ✓ to save.

Note You can only add up to eight cards.

To add to a new menu in a system-defined card:

a) Scroll using the < and > icons to select a system-defined card.
b) Click ✎ to enter the menu name. Click ✓ to save.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

To add to a system-defined menu in a system-defined card:

a) Select the menu by clicking on it. The selected menu is highlighted in a red box.

Note You can only add up to seven menus in each card and in each menu up to five tabs.

Step 5 Click **Save**.

Sort and Search Third-party User Interface

Complete the following procedure to sort the list of third-party user interfaces and to search for specific user-interfaces.

Procedure

Step 1 In **Unified CCE Administration**, choose **Overview** > **Features** > **Third-party Integration**.

Step 2 On the **Manage Third-party Integration** tab, the **Name** and **Description** columns has an arrow icon in the column header. Click the arrow to sort in the ascending or descending order.

Step 3 To search for a user-interface, enter the name or description of the page in the text box in the far left corner. As you type, user-interfaces that match your search term appear.

Delete Third-party User Interface

Complete the following procedure to delete a third-party user interface.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Features** > **Third-party Integration** > **Manage Third-party Integration**.

Step 2 Hover the mouse pointer over the row of that third-party user interface to see the **x** icon at the end of the row. Click the **x** icon and confirm your intention to delete.
The third-party user interface is deleted from Packaged CCE.

Customize the Unified CCE Administration Layout

In Unified CCE Administration, choose **Overview** > **Features** > **Third-party Integration** > **Manage Layout**.

From the Manage Layout page you can:

- Add a third-party user interface to the menu you select or create.

Note The third-party user interface is always added as a new tab in the menu.

- Add up to eight new cards, and in each card up to seven menus, and in each menu up to five tabs. You can add up to 100 third-party user interfaces to Unified CCE Administration.

Note You cannot add a third-party user interface to the following menus: Inventory, Deployment Settings, and Device Configuration menus in the Infrastructure Settings card, Third-party Integration menu in the Features card, Email and Chat menu in the Email and Chat card, Resources menu in the Desktop Settings card.

- While creating a card, enter a title and choose the color and icon from a pre-defined list. For details, see Manage User-Defined Cards , on page 225
- Add, rename, and delete menus in system-defined cards. For details, see Manage System-Defined Cards , on page 226

Note Color, name, and title of system-defined cards are not customizable.

- Drag and drop the user-defined cards in the order in which you want them to appear in the Unified CCE Administration layout.

Manage User-Defined Cards

Complete the following procedure to add new cards and menus.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Features** > **Third-party Integration**. The **Manage Layout** page displays all the cards.

Step 2 To add a new card:

a) Click the **Add New Card** card.

Note The **Add New Card** card is disabled after you have added eight cards.

b) Click ✎ to choose a color and icon for the card.

c) Click ✎ next to **Add Title** to enter the card title.

d) Click **Save**.

The new card is displayed on the **Manage Layout** page.

Step 3 To edit a card, click on any of the following icons at the bottom right corner of the card.

- Click ✎ to change the icon, color, or title of the card.
- Click ☰ to add or edit a menu. To delete a menu, click 🗑.
- Click 🗑 to delete the card.

Note You cannot delete a card or menu if it contains a third-party user interface.

Note Your changes take effect on the **Overview** page after you log into **Unified CCE Administration** again.

Manage System-Defined Cards

You can add menus to system-defined cards. You can also rename or delete user-defined menus.

Procedure

Step 1 In Unified CCE Administration, choose **Overview** > **Features** > **Third-party Integration**. The **Manage Layout** page displays all the cards.

Step 2 To add a menu to the card:

Note You cannot add more than seven menus to a card.

a) Click ☰ at the bottom right corner of the card.
b) In the **Manage Menus** page, click ✎ next to **Add Menu**.
c) In the text box that appears, enter the menu name.
d) Click ✓ to save the menu. Or click **x** to cancel.
e) Click **Done**.

Step 3 To rename or delete a menu:

Note Only user-defined menus can be renamed or deleted.

a) Click ✎ to rename the menu or click 🗑 to delete.
b) Click **Done**.

Note Your changes take effect in the **Overview** page when you log into **Unified CCE Administration** again.

Email and Chat

Email and Chat

Enterprise Chat and Email (ECE) is an optional feature that provides email and chat functionality to the contact center. To configure ECE from Unified CCE Administration, you need to add ECE Web Server into the **Inventory** page as an external machine. For more information, see Add External Machines.

In **Unified CCE Administration**, choose **Overview** > **Email and Chat** to configure the email and chat functionality.

Configuration Tasks
Configure Email and Chat

Bulk Imports

Manage Bulk Jobs

Bulk jobs are a fast and efficient way to enter data at initial setup and to incorporate large-scale changes, such as changing agent skill groups between shifts and incorporating a new contact center with multiple new agents.

Changes to an individual record are made directly to that record, using the appropriate tool (Agent, Dialed Number, and so on).

Although bulk job content files create records explicitly, they also implicitly create related records, as follows:

- An agent bulk job content file contains cells for agent team, skill groups, and attributes. Entering content in those cells creates those objects if they do not exist.
- A dialed number bulk job content file contains cells for call type. Entering content in those cells creates those objects if they do not exist.

Important Run bulk jobs:

- Only during off-peak hours. Do not run bulk jobs during heavy call load.
- Only when the Sync Status is **In Sync** for all the devices.

Supervisors have no access to the Bulk Jobs tool.

Download Bulk Job Content File Template

Bulk jobs apply changes entered in content file templates. Content file templates are in .csv format.

The content file is syntactically validated before the bulk job is created. Database-related errors and conflicts are reported during execution of the job.

Note If you are using the Packaged CCE Lab deployment, you can download the Inventory content file. Use this file to enable the System Inventory and certain features, by providing machine information and credentials.

Procedure

Step 1 Navigate to **Unified CCE Administration** > **Overview** > **Bulk Import** to open the **List of Bulk Jobs** page.

Step 2 Click **Templates**.

The **Download Templates** popup window opens.

Step 3 Click the **Download** icon for the template you want to use.

Step 4 Click **OK** to close the **Download Templates** popup window.

Step 5 Open the template in Microsoft Excel.

Step 6 Populate the file.

Step 7 Save the populated file locally.

Related Topics

Inventory Content File

Content File Rules

Note The rules in this section do not apply to the SSO Migration content file.

For more information about using the SSO Migration content file, see the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html.

Content File Create Operations

The content file spreadsheets follow these CREATE rules:

- All columns in the spreadsheet must be present, but the cells for optional fields can be left blank.
- Rows in the file are processed sequentially. It is possible for a content file to fail at any point (at any row), in which case objects up to but not including that row are added or updated.

  If a row fails, all additions or updates before that row succeed, but all subsequent create and update operations fail.
- **Agent:** Creating an agent with the following cells populated implicitly creates the objects if they do not exist: agent team, skill group, attributes, supervisor team, and department.
- **Dialed number:** Creating a dialed number with the call type and department populated implicitly creates those objects, if they do not already exist.

Content File Update Operations

The Content file spreadsheets follow these UPDATE rules:

- Enter a value in a field to change the existing value.
- Leave a field blank to keep the existing value.
- Enter ~ in a field to clear the value in the existing value.

Bulk Agent Content File

The content file for the agent bulk job contains the fields detailed in the table below.

Note Ensure that the number of agent records do not exceed 1000.

Field	Required?	Description
operation	yes	Enter one of the following (case-insensitive): • CREATE • UPDATE
agentID	no	Enter a unique string of up to 11 digits. AgentID is automatically generated if you leave the field blank. In an UPDATE operation: • You cannot change agentID • If you leave the field blank, the userName must reference an existing agent
userName	yes	Enter up to 255 ASCII characters. The login name supports the use of all characters from 33 to 126 in the ASCII character set, except for the following: double quotation mark ("), forward slash (/), backward slash (\), square brackets ([ ]), colon (:), semicolon (;), pipe (|), equal to (=), comma (,), plus sign (+), asterisk (*), question mark (?), angle brackets (< >), hash (#), percent (%), and SPACE. For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username. For supervisors who are not enabled for single sign-on (SSO), the Active Directory username must be in the user@domain format.
firstName	yes	Enter a maximum of 32 characters.
lastName	yes	Enter a maximum of 32 characters.
password	no	Enter a maximum of 256 ASCII characters. Password is case-sensitive. If SSO is enabled, the password is not saved. The default *Minimum Password Length* has been set in **Call Settings** > **Miscellaneous** (see Global, on page 210).
loginEnabled	no	Indicates whether the agent is able to log in to the agent desktop. If not specified, defaults to True.
ssoEnabled	no	Indicates whether single-sign on is supported at the agent level. This field takes effect only when the global level of SSO is mixed.
description	no	Enter up to 255 characters to describe the agent. If description is left blank during a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.

Field	Required?	Description
agentStateTrace	no	Indicates whether agent state trace is enabled for this agent. Defaults to False.
agentDeskSettingsName	no	Enter the desk settings associated with this agent. In a CREATE operation, your entry of agentDeskSettingsName generates an error when there is no desk settings with that name. Leaving this blank applies the System Default Desk Settings.
agentTeamName	no	Enter the team in which this agent is a member. In a CREATE operation, your entry of agentTeamName creates that team if it does not already exist. It appears in the List of Teams with the description BulkJob ID ####, where #### is the number of the bulk job.
skillgroup(s)	no	Enter the skill groups with which this agent is associated, delimited by the ";" character. For example: sales;billing;support. In a CREATE operation, your entry of skillgroup creates that skill group if it does not already exist. It appears in the List of Skill Groups with the description BulkJob ID ####, where #### is the number of the bulk job.
defaultSkillGroup	no	Enter the default skill group associated with this agent. If the field is specified, it must reference a skill group defined for the agent. In an UPDATE operation, an error is generated if the value is no longer one of the agent's skill groups.

Field	Required?	Description
attributes	no	These fields are name = value pairs delimited by the ";" character, where = value is optional for existing attributes. For example, english=true;sales=7. Adding an attribute with a data type (Boolean or Proficiency) and a value (true or 9), either directly in the Attributes tool or with a bulk job, defines and protects the data type and establishes that value as the default. If an attribute does not yet exist in the Attributes tool, entering an attribute name without a value generates an error. For example if english is not yet an attribute, then english returns an error. You cannot change the data type, but you can change the value. If english was created as True, entering english retains the True value in a bulk update. You can also enter english=false, which sets the agent attribute value to False, leaving the attribute default value at True. You cannot enter english=10. To clear an agent's attribute value and reestablish the attribute default on a bulk update, just specify the attribute name, for example, english. In a CREATE operation, your entry of attribute creates that attribute if it does not already exist. It appears in the List of Attributes with the description BulkJob ID ####, where #### is the number of the bulk job.
supervisor	no	Indicates whether the agent is a supervisor. Defaults to False.
supervisorTeams	no	Enter names of teams that will be supervised by this supervisor, delimited by the ";" character. For example: team1;team2;team3. Populating this field but leaving supervisorUserName blank generates an error. In a CREATE operation, your entry of supervisorTeams creates that team if it does not already exist. It appears in the List of Teams with the description Bulk Job ID: ####, showing the number of the bulk job.
siteName	no	The site name for this dialed number. If specified, the value must match an existing site name. If not specified, this field is set to default Main site.
ecePerson	no	Indicates whether the agent is a ECE enabled. Defaults to False.
screenName	yes, if ecePerson is entered	
emailAddress	no	The email address of the ECE-enabled agent. Maximum length is 50 characters.

Field	Required?	Description
peripheralSetName	yes	**Note** This field is available only for Packaged CCE 4000 agent and 12000 agent deployments. The peripheral set name for this agent. The value must match an existing peripheral set name configured for the site specified in the siteName column. In an UPDATE operation, you cannot change peripheralSetName. In a DELETE operation, you cannot delete peripheralSetName.

Related Topics

Content File Rules, on page 228

Bulk Dialed Number Content File for 2000 Agent Deployments

The content file for the dialed number bulk job contains these fields:

Field	Required?	Description
operation	yes	Enter one of the following (case-insensitive): • CREATE • UPDATE • DELETE
dialedNumberString	yes	The dialedNumberString for this dialed number. Enter a string value that is unique for the routing type, maximum of 25 characters. Valid values are alphanumeric, +, and @. **Note** You cannot update dialedNumberString.

Field	Required?	Description
routingType	yes	The routing type for this dialed number. Values are 1 to 7. • 1 (External Voice): Dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). • 2 (Internal Voice): Dialed number strings that can be called from a Cisco Unified Communications Manager phone. • 3 (Outbound Voice): Dialed number strings that are used by the Cisco Outbound Option Dialer. • 4 (Multichannel 1). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 5 (Multichannel 2). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 6 (Multichannel 3). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 7 (Post Call Survey). Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). Multichannel routing types are available only if you have configured the peripherals for Enterprise Chat and Email, SocialMiner, and/or Third Party Multichannel using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory. The order in which peripherals for these machines appear on the **Peripheral Gateways** tab (**Overview** > **Infrastructure Settings** > **Peripheral Gateways**), determines the routingType number (4, 5, or 6) for the machine. For example, if SocialMiner peripheral appears first on the tab, it is routingType 4. See the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html for information about configuring the peripherals using Peripheral Gateway Setup.
description	no	The description for this dialedNumberString. Enter a maximum of 255 characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.

Field	Required?	Description
callTypeName	no	Enter a name for the call type using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric. In a CREATE operation, your entry of callTypeName creates that call type if it does not already exist. It appears in the List of Call Types with the description BulkJob ID ####, where #### is the number of the bulk job.
mediaRoutingDomainName	yes, for routingType 4, 5, and 6	Optional for routingTypes 1, 2, and 3. If supplied, must be Cisco_Voice. Required for routingTypes 4, 5, and 6. The value must be Cisco_Voice or match an existing Media Routing Domain name.
departmentName	no	The department for this dialed number. A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID ####, where #### is the number of the bulk job. If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.
siteName	no	The site name for this dialed number. If specified, the value must match an existing site name. If not specified, this field is set to default Main site.
ringtoneMediaFileName	no	**Note** Use this field when the routing type is External Voice. Enter the custom ringtone filename. Enter a maximum of 255 characters without any spaces.
pcsEnabledDialedNumberPatterns	no	**Note** Use this field when the routing type is Post Call Survey. Enter Post Call Survey dialed number in the dialedNumberString field. Enter one or more dialed number patterns of routing type External Voice. Enter maximum of 512 characters. You can have a space-separated list of dialed numbers.

Related Topics

Content File Rules, on page 228
System Inventory for Packaged CCE 2000 Agents Deployment

Bulk Dialed Number Content File for 4000 and 12000 Agent Deployments

The content file for the dialed number bulk job contains these fields:

Field	Required?	Description
operation	yes	Enter one of the following (case-insensitive): • CREATE • UPDATE • DELETE
dialedNumberString	yes	The dialedNumberString for this dialed number. Enter a string value that is unique for the routing type, maximum of 25 characters. Valid values are alphanumeric, +, and @. **Note** You cannot update dialedNumberString.

Field	Required?	Description
routingType	yes	The routing type for this dialed number. Values are 1 to 7. • 1 (External Voice): Dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). • 2 (Internal Voice): Dialed number strings that can be called from a Cisco Unified Communications Manager phone. • 3 (Outbound Voice): Dialed number strings that are used by the Cisco Outbound Option Dialer. • 4 (Multichannel 1). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 5 (Multichannel 2). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 6 (Multichannel 3). Requests that come from Enterprise Chat and Email, SocialMiner, or third party. • 7 (Post Call Survey). Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP). Multichannel routing types are available only if you have configured the peripherals for Enterprise Chat and Email, SocialMiner, and/or Third Party Multichannel using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory. To determine the routingType number (4, 5, or 6) for each peripheral, see the chapter *Routing Type API* in the *Cisco Packaged Contact Center Enterprise Developer Reference* at https://d1nmyq4gcgsfi5.cloudfront.net/site/packaged-contact-center/documentation/. See the *Cisco Packaged Contact Center Enterprise Features Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html for information about configuring the peripherals using Peripheral Gateway Setup.
description	no	The description for this dialedNumberString. Enter a maximum of 255 characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.

Field	Required?	Description
callTypeName	no	Enter a name for the call type using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric. In a CREATE operation, your entry of callTypeName creates that call type if it does not already exist. It appears in the List of Call Types with the description BulkJob ID ####, where #### is the number of the bulk job.
mediaRoutingDomainName	yes, for routingType 4, 5, and 6	Optional for routingTypes 1, 2, and 3. If supplied, must be Cisco_Voice. Required for routingTypes 4, 5, and 6. The value must be Cisco_Voice or match an existing Media Routing Domain name.
departmentName	no	The department for this dialed number. A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID ####, where #### is the number of the bulk job. If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.
siteName	no	The site name for this dialed number. If specified, the value must match an existing site name. If not specified, this field is set to default Main site.
ringtoneMediaFileName	no	**Note** Use this field when the routing type is External Voice. Enter the custom ringtone filename. Enter a maximum of 255 characters without any spaces.
pcsEnabledDialedNumberPatterns	no	**Note** Use this field when the routing type is Post Call Survey. Enter Post Call Survey dialed number in the dialedNumberString field. Enter one or more dialed number patterns of routing type External Voice. Enter maximum of 512 characters. You can have a space-separated list of dialed numbers.

Field	Required?	Description
peripheralSetName	yes	The peripheral set name for this dialed number. The value must match an existing peripheral set name configured for the site specified in the siteName column. In an UPDATE operation, you cannot change peripheralSetName. In a DELETE operation, you cannot delete peripheralSetName.

Bulk Call Type Content File

The content file for the call type bulk job contains these fields:

Field	Required?	Description
operation	yes	Enter one of the following (case-insensitive): • CREATE • UPDATE • DELETE
name	yes	Enter a name for the call type using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric.
description	no	The description for this call type. Enter a maximum of 255 characters. There is no restriction on characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.
serviceLevelThreshold	no	Maximum time in seconds that a caller should wait before being connected with an agent. Enter a value in seconds, using positive 32-bit integers only.
serviceLevelType	no	Indicates how the system calculates the service level: • 1 = Ignore Abandoned Calls • 2 = Abandoned Calls have Negative Impact • 3= Abandoned Calls have Positive Impact If not specified, this field is set to the system default.
bucketIntervalName	no	Identifier of the bucket interval, used for reporting. If specified, the value must match an existing bucket interval. If not specified, this field is set to the system default.

Field	Required?	Description
departmentName	no	The department for this call type. A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID ####, where #### is the number of the bulk job. If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.

Related Topics

Content File Rules, on page 228

Bulk Skill Group Content File

The content file for the skill group bulk job contains these fields:

Field	Required?	Description
operation	yes	Enter one of the following (case-insensitive): • CREATE • UPDATE • DELETE
name	yes	Enter a name for the skill group using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric.
description	no	The description for this skill group. Enter a maximum of 255 characters. There is no restriction on characters. If the description field is left blank in a CREATE operation, it is set to the ID of the bulk job performing the CREATE operation.
serviceLevelThreshold	no	Maximum time in seconds that a caller should wait before being connected with an agent. Enter a value in seconds, using positive 32-bit integers only.
serviceLevelType	no	Indicates how the system calculates the service level: • 1 = Ignore Abandoned Calls • 2 = Abandoned Calls have Negative Impact • 3= Abandoned Calls have Positive Impact If not specified, this field is set to the system default.

Field	Required?	Description
bucketIntervalName	no	Identifier of the bucket interval, used for reporting. If specified, the value must match an existing bucket interval. If not specified, this field is set to the system default.
mediaRoutingDomainName	no	Enter a name for the Media Routing Domain using a maximum of 32 characters. Valid characters are period(.), underscore (_), and alphanumeric. The first character must be alphanumeric. If specified, the value must match an existing Media Routing Domain name. If not specified, this field is set to Cisco_Voice. You cannot change the mediaRoutingDomainName in an UPDATE operation. You must either leave this field blank or enter the existing mediaRoutingDomainName value.
departmentName	no	The department for this skill group. A global administrator's entry of department creates that department if it does not already exist. It appears in the List of Departments with the description BulkJob ID ####, where #### is the number of the bulk job. If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.
siteName	no	The site name for this dialed number. If specified, the value must match an existing site name. If not specified, this field is set to default Main site.
peripheralSetName	yes	**Note** This field is available only for Packaged CCE 4000 agent and 12000 agent deployments. The peripheral set name for this skill group. The value must match an existing peripheral set name configured for the site specified in the siteName column. In an UPDATE operation, you cannot change peripheralSetName. In a DELETE operation, you cannot delete peripheralSetName.

Related Topics

Content File Rules, on page 228

Add and Maintain Bulk Jobs

Procedure

Step 1 Navigate to the **Unified CCE Administration** > **Overview** > **Bulk Import** to maintain (Add, Review, and Delete) bulk jobs.

Step 2 Click **New** to open the **New Bulk Job** window.

Step 3 In the optional **Description** fields, enter up to 255 characters to describe the bulk job. See Character Sets.

Step 4 In the required **Content File** field, browse to the content file you have completed for this bulk job. The content file is validated before the bulk job is created.

Step 5 Click **Save**.

Review Bulk Job Details

To review the details for a bulk job, click the bulk job row on the **List of Bulk Jobs** page. Fields on the page are display-only.

Field	Description
ID, Description, and Type	Show the ID, description entered and type of bulk job selected when the bulk job was created.
State	Shows one of: • **Queued:** The bulk job has been queued and will process when any jobs submitted ahead of it have completed. When multiple bulk jobs are submitted, they are run in the order they are created. • **Processing:** The bulk job is being processed. To view the progress, click **Log File Download** to monitor the log file. • **Succeeded:** All operations in the bulk job were successful. • **Partially Succeeded:** Some operations were successful, and some were unsuccessful. • **Failed:** All operations were unsuccessful. • **Cancelled**: A bulk job is canceled when the preceding bulk job is terminated due to unrecoverable error while this job was in the queued state.

Field	Description
Host	The hostname of the AW server where the bulk job was initiated and will be stored. When deleted, bulk job content files and log files will be deleted from this host.
Created	The time the bulk job was submitted.
Started	The time the bulk job entered the processing state.
Finished	The time the bulk job completed or failed (left the processing state).
Total Time	The time the bulk job spent in the processing state. This is calculated as Finished - Started.
Content File	Click **Download** to open the Content .csv file that was submitted for this bulk job. You must authenticate to open or save this file. If your deployment includes two AW hosts, this button is disabled if the bulk job was created using Unified Web Administration on a host that is different from the host on which the job is being viewed.
Log File	Click **Download** to open the log file for this bulk job. If the job is still processing, click Download again to the review updates the job progresses. You must authenticate to open or save this file. If your deployment includes two AW server hosts, this button is disabled if the bulk job was created using Unified CCE Administration on a host that is different from the host on which the job is being viewed. A log file is generated for each bulk job. The log file is retained until the bulk job is deleted and contains detail of each operation that was run, as well as a summary indicating if the bulk job completed successfully or had failures.

Capacity

Capacity Info

In **Unified CCE Administration**, click **Capacity** in the left navigation menu to see a table that provides following system capacity information:

Column	Description
Status	The status column shows where your system stands with respect to the capacity limit. The status icons are: • Green for 0-75% of capacity. • Yellow for 76-95%. • Orange for 96-99%. • Red for when you are at 100%.
Number of Configured	Shows the name of the object.
At Most	Shows the maximum capacity of each configurable object that is allowed.
Actual	Shows the number of objects currently configured on your system.
% Used	Shows the percentage of the maximum capacity represented by your configuration.