



Packaged CCE Administration

- [Getting Started](#), on page 1
- [Smart License](#), on page 10
- [Specific License Reservation](#), on page 30
- [Infrastructure Settings](#), on page 34
- [User Setup](#), on page 76
- [Organization Setup](#), on page 98
- [Desktop Settings](#), on page 136
- [Call Settings](#), on page 181
- [Feature Setup](#), on page 219
- [Email and Chat](#), on page 243
- [Bulk Imports](#), on page 244
- [Capacity](#), on page 260

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 117

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 86).

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 188).



Remember Not all tools are available for all Deployment Types.

Tool	Editable Fields
Administrators	All fields
Agents	<p>All fields except Site and Peripheral Set.</p> <p>If an agent is not enabled for single sign-on, you can check Change Password to reset the agent's password.</p> <p>Note</p> <ul style="list-style-type: none"> • 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	<p>Name</p> <p>You cannot edit the built-in bucket interval.</p>
Bulk Jobs	No fields
Business Hours	<p>General tab: All fields.</p> <p>Regular Hours tab: All fields.</p> <p>Special Hours & Holidays tab: All fields.</p> <p>Status Reasons: The Status Reason field is editable.</p>
Call Types	All fields except the system-generated ID.
Campaigns	<p>General tab: All fields except Type field.</p> <p>Skill Group tab: You can add and delete the Skill Groups using Add and Delete buttons.</p> <p>Advanced tab: All fields.</p>

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	<p>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.</p> <p>When you delete an agent, the association with team is also removed and same is updated in the corresponding collection in Unified Intelligence Center.</p>
Attributes	Marked	—
Bucket Intervals	Marked	—
Bulk Jobs	Permanent	<p>Deletes the bulk job, its content file, and its log file from the host computer that created it.</p> <p>You can delete a bulk job that is in queue, has completed, or has failed.</p> <p>You cannot delete a bulk job that is in process.</p> <p>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.</p>

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 choose 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
- Cisco Virtualized Voice Browser (VVB) and

- Cloud Connect Publisher

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 and VVB) or a Differential sync.

Full Sync: This option is enabled for all CVPs (Main site and remote site) and VVBs (Main site and remote site).

Full Sync does the following:

- CVP: 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.
- VVB: synchronizes all configuration data from the time when the initial configuration was done. Use this option after you reimage, reinstall, or readd the VVB Server.
- Cloud Connect: synchronizes all configuration data from the time when the initial configuration was done. Use this option after you reimage, reinstall, or read the Cloud Connect Publisher.

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

-
- 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.

Smart License

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.

Related Topics

[License Management](#), on page 28

[Prerequisites for Smart Licensing](#), on page 12

[Smart License Deployments](#), on page 13

[Evaluation Mode](#)

[Select License Type](#), on page 15

[Registration, Authorization, and Entitlement Status](#), on page 18

[Out-Of-Compliance and Enforcement Rules](#), on page 20

[Smart Licensing Task Flow](#), on page 14

[Obtain the Product Instance Registration Token](#), on page 14

[Configure transport settings for smart licensing](#), on page 15

[Register with Cisco Smart Software Manager](#), on page 17

[Smart Licensing Tasks](#), on page 28

[Renew Authorization](#), on page 29

[Renew Registration](#), on page 29

[Reregister License](#), on page 29

[Deregister License](#), on page 30

Smart Licensing Capabilities

Smart Licensing works in conjunction with Cisco Smart Software Manager (Cisco SSM) to intelligently manage product licenses by providing real-time visibility of license status and usage. You can use this data to make better purchase decisions, based on your consumption. Smart Licensing establishes a pool of software licenses or entitlements in Cisco Smart Account.

The Smart Account provides a central location where you can view, store, and manage your licenses, across the organization. You can get access to your software licenses, hardware, and subscriptions through your Smart Account. Smart Accounts are required to access and manage Smart License-enabled products.

Creating a Smart Account is easy and takes less than five minutes. [Create a Smart Account](#) on software.cisco.com.

Documentation Resources

Table 1: Documentation Resources

For	Go to...
Smart Licensing Prerequisites	Prerequisites for Smart Licensing, on page 12
Understanding the License consumption Calculation	License Consumption Calculation, on page 23
Migration to Smart Licensing	Migrate to Smart Licensing, on page 25
Smart Licensing tasks in SPOG/OAMP	Smart Licensing Task Flow, on page 14
Best Practices	Best Practices, on page 30

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-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 13](#).

- **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`
 - `-import keytool.exe <ICM install directory>\ssl\cacerts -file <filepath>.cer -alias <alias>`
3. Enter the truststore password when prompted.
4. Enter 'Yes' when prompted to trust the certificate.
5. Restart the Tomcat service.

Related Topics

[Configure transport settings for smart licensing](#), on page 15

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>.

Smart Licensing Task Flow

Complete these tasks to set up smart licensing for Packaged CCE.

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 CCE 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 CCE 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.

Related Topics

[Obtain the Product Instance Registration Token](#), on page 14

[Configure transport settings for smart licensing](#), on page 15

[Register with Cisco Smart Software Manager](#), on page 17

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.

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 CCE and Cisco SSM.

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

Step 2 Click **Transport Settings** to set the connection method.

Step 3 Select the connection method to Cisco SSM:

- **Direct** - (Packaged CCE communicates directly with Cisco's licensing servers.)
URL: "https://smartreceiver.cisco.com/licservice/license".
This is the default option. The configured URL is displayed.
- **Licensing Transport URL** - (for SSM On-Prem)—Enter the appropriate URL in the URL field.
- **HTTP/HTTPS Proxy**-(Send data through an intermediate HTTP or HTTPS proxy.) Enter the appropriate Host Name and Port number in the respective fields.

Note Proxy servers that require authentication aren't supported for this connection method.

Step 4 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 modes—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 a 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.



Note If you select the 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.



Note If you select the Deployment Type as *ICM Rogger/Logger*, the system automatically updates to **Perpetual** even when the License Type is configured as **Flex**.

- 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.

The following table lists the license types and licenses offered as part of Unified CCE and Packaged CCE Smart Licensing:

License Type	Licenses
Flex Production	Unified CCE and Packaged CCE: <ul style="list-style-type: none"> • Standard Agent • Premium Agent • Dialer Ports • Server License

License Type	Licenses
Perpetual Production	<p>Unified CCE and Packaged CCE:</p> <ul style="list-style-type: none"> • Premium Agent • Dialer Ports • Server License <p>ICM:</p> <ul style="list-style-type: none"> • Regular Agent • Avaya PG • Third-party IVR licenses • Server License
Perpetual Non-Production	<ul style="list-style-type: none"> • Regular Agent • Premium Agent • Dialer Ports • Server License • Avaya PG

Step 4 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.

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

Step 2 Click **Register**.

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

Step 3 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 4 Click **Register** to complete the registration process.

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

Table 2: Smart Licensing Status

Smart License Status	Description
On Unsuccessful Registration	
Registration Status	Unregistered
License Authorization Status	Evaluation
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/>.

Related Topics

[Obtain the Product Instance Registration Token](#), on page 14

Registration, Authorization, and Entitlement Status

Registration Status

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

Table 3: 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 product authorization status for Smart Licensing in the Unified CCE Administration portal:

Table 4: 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 product instance license entitlement status for Smart Licensing in the Unified CCE Administration portal:

Table 5: 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.

Status	Status Description
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.
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.

License States

Smart Licensing has the following states:

- **Registration State**

- **Unregistered**—Product Instance is unregistered.
- **Registered**—After you purchase the license, you need to register the Product Instance with Cisco SSM. To register with Cisco SSM, generate a registration token from the Cisco SSM portal. Use the registration token to register your Product Instance.
- **Registration Expired**—Product Instance registration has expired because the ID Certificate issued by Cisco SSM is not renewed for more than 12 months. Reregister the Product Instance.

- **Authorization State**

- **No licenses in use**
- **Evaluation Mode**—The Product Instance license has an Evaluation period of 90 days. In the Evaluation period you have unlimited access to the product with highest set of product capabilities and unlimited number of licenses. You 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.
- **In Compliance**—When the license consumption is as per the purchased quantity, the product is compliant.
- **Evaluation expired**—Product Instance evaluation period has expired.
- **Authorized**—Product Instance is in authorized or in compliance state. Authorization is renewed every 30 days.
- **Out of Compliance**—Product Instance reports license usage to Cisco SSM every 15 minutes. If your license consumption is more than the entitlements for five consecutive reporting intervals, the Product Instance is transitioned 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 transitioned to the Enforcement state.
- **Authorization Expired**—Product Instance authorization has expired. This usually happens when the product has not communicated with Cisco SSM for more than 90 days. It is in an overage period for 90 days before restrictions are enforced.

- **Enforcement State**

When the 90 day period of Out-of-Compliance, Evaluation Period or Authorization period has expired, the Product Instance is moved to the Enforcement state in which system operations are impacted for Contact Center components. 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.

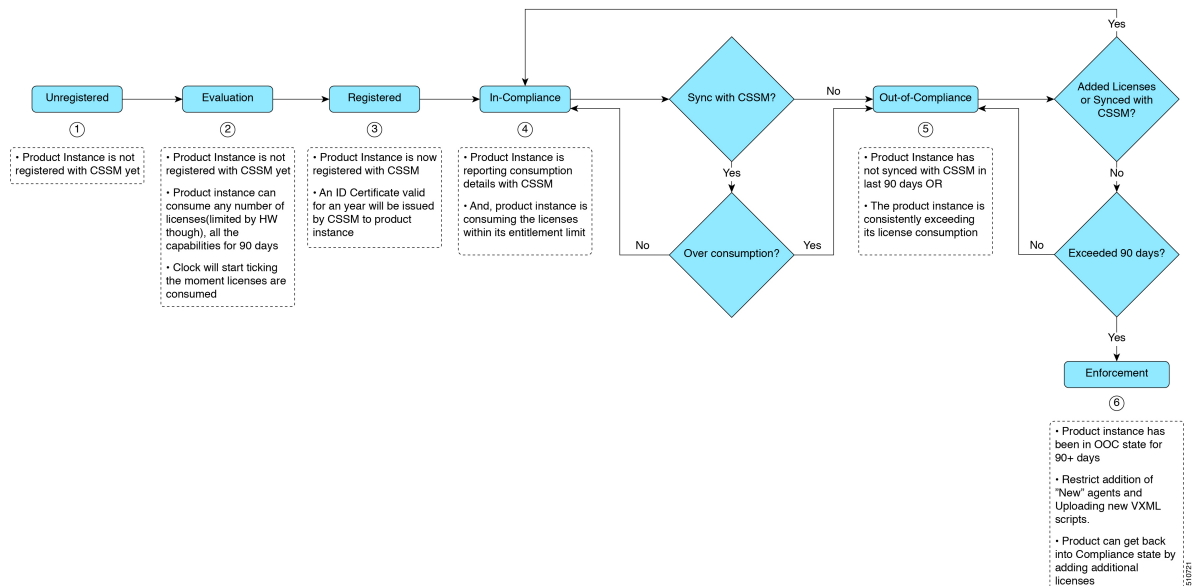
Renew the license authorizations to exit the Authorization expiry state.

- **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.

A pictorial representation of different license states is as follows:

Figure 1: License States



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.

License Consumption Calculation

The system reports peak license usage to Cisco SSM every 15 minutes. If in five consecutive reports you are seen to have consumed more licenses than you are authorized to, 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 additional licenses. If you do not take corrective action within the 90 days period, the Product Instance is pushed to the Enforcement state in which, some of the operations are impacted.

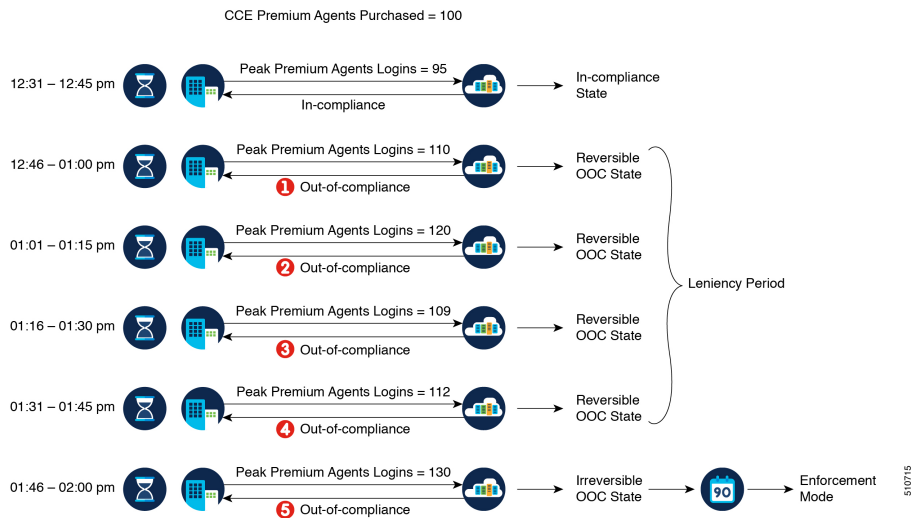
Log in to Cisco SSM to view the detailed license consumption. Cisco SSM reports purchased quantity, in-use quantity, and balance licenses. At a quick glance, you can decide if the consumption of your licenses are in deficit or surplus, based on which you can make the right decision on the number of licenses that are required.

License Computation Scenario 1

License purchased: 100 licenses

Figure 2: License Computation

Out-of-compliance (OOC) and Enforcement Modes:



If Cisco SSM registers consecutive five instances of license over usage, the Product Instance transitions to Out-of-Compliance. Thereafter, the Product Instance reports Locked usage quantity (130 in the above scenario) until the deficit licenses (130-100=30) are purchased. The Locked usage is the highest number of license usage (130) in the Out-of-Compliance state. The Product Instance will not report the actual license usage when the Product Instance is in the Out-of-Compliance state.

Purchase additional licenses from the [Cisco Commerce website \(CCW\)](#) to exit the Out-of-Compliance state.

Reported Usage column in the **License Management** page displays the locked usage quantity. However, the actual license usage is available in the **License Consumption** report of CUIC.

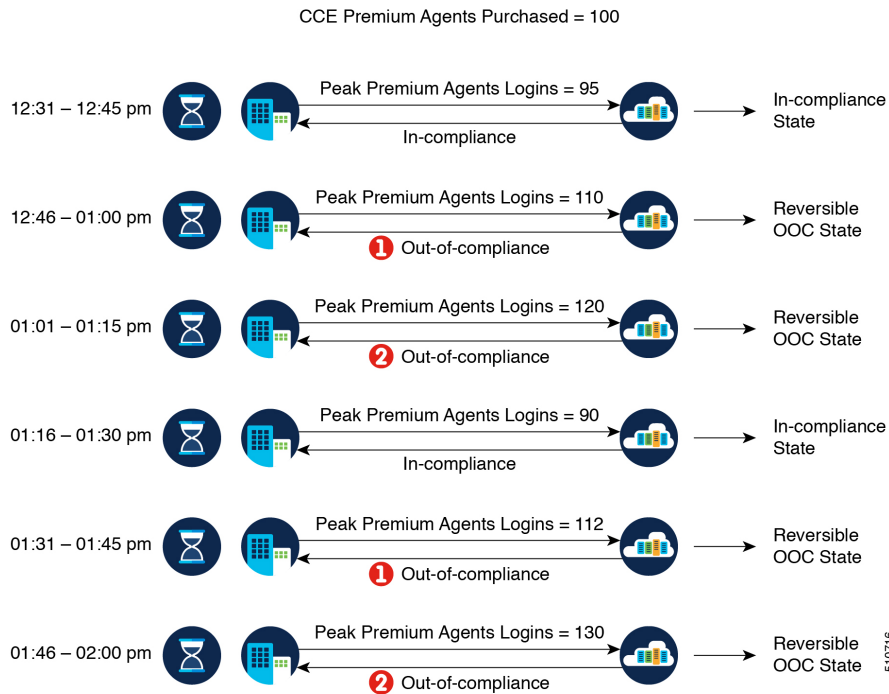
License Computation Scenario 2

If Cisco SSM reports only two consecutive instances of license over usage within a one-hour window, the Product Instance will not transition to Out-of-Compliance. For example:

License Purchased: 100 licenses

Figure 3: License Computation

Out-of-compliance (OOC) and Enforcement Modes:



In the example, the Product Instance is back to In-compliance state after two instances of overage. The next time the Product Instance goes Out-of-Compliance, the count will be 1 of 5. So, you get 45 min (after the first Out-of-Compliance notification from Cisco SSM) to bring back the consumption within the acceptable range to stay in the In-compliance state.



Note To know about the agent license that is consumed by the Standard and Premium licenses, see the *Cisco Collaboration Flex Plan Contact Center Data Sheet* at <https://www.cisco.com/c/en/us/products/collateral/unified-communications/cisco-collaboration-flex-plan/datasheet-c78-741220.html>

New Deployments

For new deployments, buy the licenses on Cisco Commerce website at <https://apps.cisco.com>. Begin to use the product by using the licenses from your Smart Account.

Migrate to Smart Licensing

If you are upgrading to Unified CCE Release 12.5(1), from Unified CCE Release 10.x or above, use self serve capabilities in [Cisco SSM](#) to declare the licenses that you own.

Use the PUT tool to electronically order the new media.



Note PUT tool is only for customers who prefer to continue to operate in Classic Licensing mode.

For Unified CVP, if you have an active SWSS contract, you can migrate your unconsumed PAKs and devices to Smart Licensing on [Cisco SSM](#) portal or [LRP \(License Registration Portal\)](#). First assign the classic PAK or PLM to the Smart Account and Virtual Account to move to Smart Licensing. To migrate from Unified CVP 10.x to Smart Licensing, upgrade to Unified CVP 11.6 and then to Unified CVP 12.5. There are two types of migration:

- PAK-Based Migration
- Device-Based Conversion

Inactive SWSS contract

If the SWSS contract is inactive, repurchase the licenses or move to Flex, and follow the steps to convert classic licenses to smart licenses.

PAK-Based Migration

Migrate to Smart Licensing for fulfilled, partially fulfilled, and unfulfilled PAKs.

1. Log in to the Traditional Licensing Portal at <https://tools.cisco.com/SWIFT/LicensingUI/Home>.
2. Locate the PAKs that are to be migrated.
3. Right click and select **Assign to Smart Account and Virtual Account**.
4. Select the Smart Account and Virtual Account to which the PAK will be assigned.

Once done, the classic PAKs will show assigned Smart Account.

Using LRP

1. Select the PAK that needs to be converted to smart entitlement.
2. From the PAK context option, select **Convert to Smart Licensing**.
3. Select the **SKUs, Quantity to Convert** and click on **Submit**.



Note Classic Licenses that are partially converted will need new Classic License file for managing the remaining Classic Licenses.

After the licenses are converted to smart entitlements, successful conversion message is shown. The entitlements will be available on Cisco SSM under selected Smart and Virtual Account.

Using Cisco SSM

Convert PAKs to equivalent Smart Licenses.

1. Go to the **Convert PAKs** tab.

Assigned PAKs are listed on the Cisco SSM portal.

2. Click **Convert to Smart License** in the **Actions** column.
3. Select **SKUs** and **Quantity to Convert** and click **Next**.

Classic Licenses which are partially converted will need new Classic License file for managing the remaining Classic Licenses.

4. Review and to confirm click **Convert License**.

Once converted to Smart Entitlement, the old classic licenses will be invalidated. Converted Smart Licenses are added into the Smart Account and the Virtual Account.

Device-Based Conversion

Use the device-based Smart Licensing to convert the Classic licenses to smart entitlements.

Using LRP

1. Login to the Traditional Licensing Portal at <https://tools.cisco.com/SWIFT/LicensingUI/Home>
2. Go to **Devices** tab and then **Add Device**.
3. Locate the device to be migrated (filter using the device UUID). Once added, the added device shows up under **Devices** tab.
4. Select the device and right click **Assign to Smart Account** to Smart Account and Virtual Account.
5. Select the Smart Account and the Virtual Account.

Once done, the table is updated with the Smart Account assigned to the device.

6. For Classic licenses to be converted to smart entitlements, select the device and select **Convert licenses to Smart Licensing** option.
7. Select the SKUs and **Quantity to Convert**.

Classic Licenses which are partially converted will need new Classic License file for managing the remaining Classic Licenses.

8. Confirm and click **Submit**.

Once the licenses are fully converted, the device UUID will be removed from the LRP. Once done, the successful conversion message is shown. The entitlements will now be available on Cisco SSM under selected Smart and Virtual Account.

Using Cisco SSM

Assigned Devices show up on the Cisco SSM Portal. The Cisco SSM portal is refreshed every hour. If the assigned device is not visible in Cisco SSM, please recheck after an hour.

1. Go to **Convert Licenses** tab and click the **License Conversion wizard**.
2. Select the **Product family** and provide the device UUID.
3. Select the **SKU** and **Quantity to Convert**.

Classic Licenses which are partially converted will need new License file for managing the remaining Classic Licenses.

4. Review, Confirm and click **Submit**.

When the conversion is complete and smart licenses are active, the classic licenses are invalidated.

License Management

Smart Licensing can be managed by using Cisco SSM and .

- **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.

Related Topics

[Configure transport settings for smart licensing](#), on page 15

[Register with Cisco Smart Software Manager](#), on page 17

[Select License Type](#), on page 15

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.

Related Topics

[Renew Authorization](#), on page 29

[Renew Registration](#), on page 29

[Reregister License](#), on page 29

[Deregister License](#), on page 30

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.

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

Step 2 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.

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

Step 2 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 CCE 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.

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

Step 2 Click **Action > Reregister**.

Step 3 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 4 Click **Reregister** to complete the reregistration process.

Step 5 Close the window.

Deregister License

Use this procedure to deregister Packaged CCE 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 CCE 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 it.

-
- Step 1** In Unified CCE Administration, navigate to **Overview > Infrastructure Settings > License Management** .
- Step 2** Click **Action > Deregister**.
- Step 3** On the **Confirm Deregistration** dialog box, click **Yes** to deregister.
-

Best Practices

Some of the best practices for Smart Licensing are:

- Before purchasing your licenses, run the License Consumption report on the existing system to understand the consumption pattern to make the right purchase decisions on the license requirement.
- Configure Admin email address in Cisco SSM to receive notifications and alerts from Cisco SSM.

Specific License Reservation

Devices (product instances of Unified CCE) that register with Smart Licensing have to share the license information with Cisco Smart Software Manager (Cisco SSM) at regular intervals. Your deployments that cannot periodically share license utilization data with Cisco SSM or due to regulatory reasons can use the Specific License Reservation feature. Cisco offers license reservation as an on-request configuration for such product instances.

You can reserve licenses (including add-on licenses) for your product instance on Cisco SSM. Specific License Reservation is enabled through the option **License Management** in the Unified CCE Administration Console.



Note The reserved licenses require no renewal or reauthorization unless there is a license usage change on the device. License reservation provides limited functionality to certain Smart Licensing features such as transfer of licenses between products, license usage, and asset management.

The Specific License Reservation (SLR) feature does not offer the following benefits that are available as part of the Smart Licensing feature:

- Dynamic movement of license consumption between products
 - Real-time license usage visibility and asset management
 - Simplified product registration
-

Task Flow for SLR

For Specific License Reservation (SLR), you can perform the following tasks:

- **Enable Reservation**—You will be able to enable reservation to initiate the **License Reservation** process.
- **Request License Reservation**—You will be able to raise the request for reservation code to reserve the number of licenses required.
- **Update License Reservation**—You will be able to generate the authorization code and confirmation code to update the reserved license.
- **Return License Reservation**—You will be able to generate the return code to remove the reserved license.



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.

Enable Reservation

After getting approval from Cisco, use the following procedure to enable reservation on a product instance.

Before you begin

Ensure that the product instance is in the unregistered state and the connection is not active.

- Step 1** In the Inventory page, navigate to **Infrastructure Settings > License Management**.
- Step 2** Click **License Settings**, and check the **Enable Reservation** checkbox.
- Step 3** Click Save.
The *Saved successfully* message appears on the **Select License Settings** window.

Note After you have enabled reservation, the **Disable Reservation** option is available to reset the *License Type* to default.

License Type is not applicable for PLR.

Request Reservation Licenses

Before you begin

After you have enabled a reservation, follow the procedure to request the reservation code:

Step 1 In the Inventory page, navigate to **Infrastructure Settings > License Management > Register**.

Step 2 The **Reserve Licenses** window appears. Follow the steps in the window:

- a) Click **Request Reservation Code**, and copy the code from the text box.
- b) Click Cisco Smart Software Manager (CSSM) link in step 2.
The Smart Software Licensing page appears.
- c) Click **License Reservation** tab.
Smart License Reservation page pops-up.
- d) Paste the **Request Reservation Code** that you copied in Step 2a into the text box. Click **Next**.
Smart License Reservation page displays Product Instance Details.
- e) Under **Licenses to Reserve**, select the required radio button.
Depending on the selection, the product instance details display the license information. Fill in the required details, and click **Next**.

The Smart License Reservation page displays the filled information.

- f) Click **Generate Authorization Code**.
Smart License Reservation page displays the Authorization Code.
- g) Click **Copy to Clipboard**. A confirmation message appears.
In the Unified CCE Administration console, **Reserve Licenses** window, paste the code in the **Authorization Code** text box. Click **Reserve**.

Note You can download the Authorization Code for future reference.

Step 3 **Successfully Completed** message appears on the **Reserve Licenses** window.

Step 4 **Close** the window.

On completion, in the **License Management** screen you will see the **License Authorized Status** in green.

Return Reservation Licenses

Before you begin

When you want to return the licenses, use the following procedure to return the license reservation on a product instance.

Step 1 In the Inventory page, navigate to **Infrastructure Settings > License Management > Action**.

- Step 2** In the drop-down list, choose **Return**.
The **Return Reservation** window appears.
- Step 3** In the **Return Reservation** window, paste the **Authorization Code** which you had generated for the specific license.
Generates a **Return Code**.
In Cisco Smart Software Manager (CSSM) page, click **Product Instance**.
The page displays the list of licenses. Use the search text box to select the specific license.
- Step 4** In the **Action** tab beside the specific license, click on the downward arrow. Select **Remove**.
Remove Product Instance page appears.
- Step 5** In the **Remove Product Instance** page, enter the return code in the **Return Reservation** window and close the window.
- Step 6** In the **License Management** page, click the **License Setting** tab.
- Step 7** In the **Select License Settings** window, uncheck the **Enable Reservation** check box, and click **Save** and close the window.
In the License Management page, the **Smart Licensing Status** is **Unregistered**.
-

Update Reservation Licenses

Before you begin

When you want to update the specific license reservation, you must generate the authorization code in the Cisco Smart Software Manager (CSSM) page. Follow the procedure to create the authorization code, and to update the specific license:

If you reserve PLR, you will not be able to update the reservation.

- Step 1** In the CSSM page, click the **Product Instance** tab.
- Step 2** Use the search text box to search the specific license you want to modify.
- Step 3** In the **Action** tab, beside the name of the license, click the downward arrow, and choose **Update Reservation Licenses**.
- Step 4** The **Update License Reservation** window appears.
- Step 5** Fill in the details and click **Next**.
- Step 6** Select the radio button beside **Reserve a specific license**.
- Step 7** Fill in the required license details, and click **Next**.
Fill in all the required details, and click **Generate Authorization Code**. Click **Copy to Clipboard**.
- Step 8** In the Inventory page, navigate to **Infrastructure Settings > License Management > Aciton > Update Reservation**.
- Step 9** The **Update Reservation** window appears. In the **Authorization Code** text box, paste the authorization code. Click **Update**.
- Step 10** The **Confirmation Code** text box displays the confirmation code. Copy the code.
- Step 11** In the CSSM **Update License Reservation** page. Click **Enter Confirmation Code**.
The **Enter Confirmation Code** window appears.
- Step 12** In the **Reserve Confirmation Code** text box, enter the confirmation code that is generated in the **Update Reservation** window. Click **OK**.
A message confirms that the license is reserved successfully.
-

Infrastructure Settings

Inventory Management

Inventory update can be done in the following scenarios:

- When you rebuild Virtual Machines (VMs), you can update the IP address or hostname of these machines in the inventory.
- When you move your existing VMs to another data center, you can update the IP address or hostname of these machines in the inventory.

For more information, see:

- [Update IP Address or Hostname](#) for 2000 Agent deployments
- [Update IP Address or Hostname](#) for 4000 or 12000 Agent deployments

Manage Devices

You can configure any of the following components:

- CVP Server
- CVP Reporting Server
- VVB
- Finesse
- Identity Service

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

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 6: 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.

Field	Required?	Description
Enable secure communication with VRU PIM	-	Enables secure communication between ICM and the Unified CVP Server.
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

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 7: IVR Service Configuration Settings

Field	Required?	Description
Use Security for Media Fetches	-	<p>If you select No (default), the HTTP URLs are generated to the Media Servers.</p> <p>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.</p> <p>Select Yes to generate the HTTPS URLs to the Media Servers.</p>
Use Backup Media/VXML Servers	-	<p>If you select Yes (default) and a Media Server is unavailable, the gateway attempts to connect to the backup Media Server.</p>
Use Host Names for Default Media/VXML Servers	-	<p>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.</p> <p>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.</p> <p>To enable HA for Media Server, open the mediaServer.properties file in the C:\Cisco\CVP\conf folder and configure the following:</p> <ul style="list-style-type: none"> • MediaServer.1.hostName = <Media Server Host> • MediaServer.1.ip = <Media Server IP> <p>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.</p>
Call Timeout	yes	<p>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.</p> <p>Minimum is 6 seconds. Default is 7200 seconds.</p>

Field	Required?	Description
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.

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 8. 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		
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.

Field	Required?	Description
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		
Note	This procedure is applicable for both RSA and ECDSA certificate	
Incoming Secure Port	no	Specifies the port to be used. Default is 5061.
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.

Field	Required?	Description
Supported Ciphers	no	<p>This field defines the ciphers, which is supported by Unified CVP, with key size lesser than or equal to 2048 bits.</p> <p>The default cipher is TLS_RSA_WITH_AES_128_CBC_SHA, which is prepopulated.</p> <p>Cipher configuration is available only if TLS is enabled.</p> <p>Click + (Add) to add a new cipher.</p> <p>Note At least one valid cipher is required in the Supported Ciphers list</p> <p>In case of ECDSA, add below ciphers:</p> <ul style="list-style-type: none"> • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 <p>After you add the ciphers, restart the system.</p>

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.

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 9: 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.

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 10: 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.

Configure Media Server

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

-
- 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 **Anonymous** 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

-
- Step 1** Navigate to **FTP server** that you have created in **Connections** tab.
 - Step 2** Goto **Actions** tab and click **Basic Settings**.
 - Step 3** Click **Connect As**.
 - Step 4** Choose **Application User (pass-through authentication)** option and click **OK**.
 - Step 5** Click **OK** in **Edit Site** window.
-

Configure Unified CVP Reporting Server

Reporting provides historical reporting to a distributed self-service deployment in a call center. The Unified CVP Reporting Server receives the reporting data from one or more Unified CVP Servers and Unified 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 Unified CVP Call Servers can send data to a single Unified CVP Reporting Server.

Reporting Server Users and Passwords

You can manage Reporting Server Users and Passwords using Windows Operating System Local User Management. However, before changing users and passwords, ensure that you stop the Cisco CVP CallServer, Cisco CVP SNMP Management, and Informix IDS CVP services. Don't stop the Cisco CVP WebServicesManager service.

To manage Reporting Server users and passwords, use the **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 Unified 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 running this command.

4. Verify if the *reporting.properties* file is updated. The passwords for **cvp_dbadmin** and **cvp_dbuser** are encrypted.
5. Restart the Unified CVP Reporting server and access the Unified 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

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 11: Reporting Server Properties

Field	Required?	Description
Trunk Utilization		

Field	Required?	Description
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

SUMMARY STEPS

1. Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Reporting Server**.
2. Click the **Database Configuration** tab. Complete the following fields:
3. Click **Save**.

DETAILED STEPS

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 12: 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

SUMMARY STEPS

1. Navigate to **Unified CCE Administration > Overview > Infrastructure Settings > Device Configuration > CVP Reporting Server**.
2. Click the **Infrastructure** tab. Complete the following fields:
3. Click **Save**.

DETAILED STEPS

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 13: 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.

Field	Required?	Description
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		
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.

-
- 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:
- 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.
 - 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).

- 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. This procedure is applicable for both RSA and ECDSA certificate		
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.

Field	Required ?	Description
Cipher Configuration	Yes	<p>Note Enable TLS(SIP) to use this security parameter.</p> <p>The default cipher <code>TLS_RSA_WITH_AES_128_CBC_SHA</code> is available in the Cipher Configuration list. The default cipher is mandatory for TLS version 1.2 and cannot be deleted.</p> <p>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).</p> <p>b. Click Add</p> <p>In case of ECDSA, add below ciphers:</p> <ul style="list-style-type: none"> • <code>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</code> • <code>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</code> <p>After you add the ciphers, restart the system.</p>
SRTP	-	<p>Note Enable TLS(SIP) to use this security parameter.</p> <p>By default, SRTP is disabled.</p> <p>Enable SRTP to secure media on the IVR leg. When SRTP is enabled, the IVR media is encrypted. SRTP uses Crypto-Suite <code>AES_CM_128_HMAC_SHA1_32</code> for encrypting the media stream.</p>
Allow RTP(Mixed Mode)	-	<p>Note Enable TLS(SIP) and SRTP to use this security parameter.</p> <p>Allow RTP (Mixed Mode) is available when you enable SRTP.</p> <p>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.</p>

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>

- 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		
Configured ASR Servers	No	<p>a. Click the '+' icon and enter the hostname or IP address of ASR server.</p> <p>b. Click Add.</p>
TTS Servers		
Configured TTS Servers	No	<p>a. Click the '+' icon and enter the hostname or IP address of TTS server.</p> <p>b. Click Add.</p>

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

- 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 Comprehensive .
Sigdigits	No	<p>Enter the number of digits that are used as the significant digits. Range is 0 to 20.</p> <p>The call arrives at Unified CVP with the significant digits (SigDigit) prepended to the Dialed Number (DN). Unified CVP strips the digits and transfers the call to the Unified ICM. When ICM returns the label to Unified CVP to route the call to Cisco VVB, Unified CVP prepends the digits again. The Cisco VVB uses the SigDigit configuration on the Comprehensive application to remove the prepended digits so that when the IVR leg of the call is set up, the original label is used on the incoming VoiceXML request.</p>
Maximum Sessions	Yes	<p>Enter the number of sessions you like to associate with the application. Range is 1 to 600.</p> <p>Note The number of sessions must be less or equal to the license provided by Cisco VVB.</p>
Enable HTTPS	No	<p>By default, the Enable HTTPS option is disabled.</p> <p>Click to enable the option. When enabled, the communication between the Cisco VVB and VXML server is encrypted.</p> <p>If you have enabled secure communication, then ensure to:</p> <ul style="list-style-type: none"> • Upload the relevant certificate. To upload the certificate, see the Upload certificate or certificate trust list topic in <i>Cisco Unified Communications Operating System Administration Guide</i>. • Restart VVB services using the VVB Admin UI (Cisco Unified Serviceability > Tools > Control Center - Network Services) or the system CLI command "utils service restart Cisco Tomcat".

Field	Required?	Description
Configured Triggers	Yes	<p>The field contains default SIP trigger configured for the Comprehensive application. See Default SIP Triggers.</p> <p>To add a new trigger:</p> <ol style="list-style-type: none"> Click the '+' icon, and enter a new SIP trigger to be associated with the application. Valid input triggers are numbers (0-9), asterisk (*), and period (.). For example: 9191*. Note Do not create a trigger with only an asterisk or a period. If the trigger contains these characters, provide a number too. An error message appears for an invalid input. 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. <p>To remove a trigger from the list, click the 'x' icon that is associated with the trigger in the list.</p>

- To configure **Ringtone** application

Field	Required?	Description
Application	Yes	From the Application drop-down list, choose Ringtone.
Maximum Sessions	Yes	<p>Enter the number of sessions you like to associate with the application. Range is 1 to 600.</p> <p>Note The number of sessions must be less or equal to the license provided by Cisco VVB.</p>

Field	Required?	Description
Configured Triggers	Yes	<p>The field contains default SIP trigger configured for the Ringtone application. See Default SIP Triggers.</p> <p>To add a new trigger:</p> <ol style="list-style-type: none"> Click the '+' icon, and enter a new SIP trigger to be associated with the application. Valid input triggers are numbers (0-9), asterisk (*), and period (.). For example: 9191*. Note Do not create a trigger with only an asterisk or a period. If the trigger contains these characters, provide a number too. An error message appears for an invalid input. 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. <p>To remove a trigger from the list, click the 'x' icon that is associated with the trigger in the list.</p>

- To configure **Error** application

Field	Required?	Description
Application	Yes	From the Application drop-down list, choose Error.
Maximum Sessions	Yes	<p>Enter the number of sessions you like to associate with the application. Range is 1 to 600.</p> <p>Note The number of sessions must be less or equal to the license provided by Cisco VVB.</p>
Custom error prompt	No	<p>Provide the custom error .wav file to play.</p> <p>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.</p>

Field	Required?	Description
Configured Triggers	Yes	<p>The field contains default SIP trigger configured for the Error application. See Default SIP Triggers.</p> <p>To add a new trigger:</p> <ol style="list-style-type: none"> Click the '+' icon, and enter a new SIP trigger to be associated with the application. <p>Valid input triggers are numbers (0-9), asterisk (*), and period (.). For example: 9191*.</p> <p>Note Do not create a trigger with only an asterisk or a period. If the trigger contains these characters, provide a number too.</p> <p>An error message appears for an invalid input.</p> <ol style="list-style-type: none"> Click Add. The trigger appears in the Configured Triggers list. <p>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.</p> <p>To remove a trigger from the list, click the 'x' icon associated with the trigger in the list.</p>

Step 5 Click **Save**.

Default SIP Triggers

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

Table 14: Default SIP Triggers

Application	Description	Pre-configured SIP Trigger
Comprehensive	Used for comprehensive calls	777777777*
Ringtone	Used for playing ringtone and whisper	91919191*
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.

-
- 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 57
- [Contact Center Enterprise Administration and Data Server Settings](#), on page 60
- [Cluster Settings](#), on page 62

Contact Center Enterprise CTI Server Settings

Use the Contact Center Enterprise CTI Server Settings gadget to configure the A and B Side CTI servers. All fields on this tab are populated with default system values or with values an administrator has previously entered. Change values to reflect your environment and preferences.

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

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



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

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

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



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

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

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

-
- 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 15: 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	<p>The port of the Unified CCE Administration & Data Server.</p> <p>The default value is 1433.</p> <p>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.</p>
AW Database Name	The name of the AW Database (AWDB). For example, <i>ucceinstance_awdb</i> .
Domain	(Optional) The domain name of the AWDB. For example, <i>cisco.com</i> .
Username	<p>The username required to sign in to the AWDB.</p> <p>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.</p> <p>If you do not specify a domain, this user must be an SQL user.</p>
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.

-
- 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 15: Field Descriptions, on page 61](#). 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.

-
- 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**.
-

Configure Cisco Identity Service

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

Task
Configure an Identity Provider (IdP), on page 63
Configure SAML Certificate Secure Hash Algorithm from SHA-1 to SHA-256, on page 69
Configure the Cisco Identity Service, on page 69
Set Up the External HDS for Single Sign-On, on page 72
Register Components and Set Single Sign-On Mode, on page 72
For more information about configuring the Single Sign-On feature, see <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-maintenance-guides-list.html .
Cisco SNMP Setup (optional)

Configure an Identity Provider (IdP)

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



Note For a current list of supported Identity Provider products and versions, see the [Contact Center Enterprise Compatibility Matrix](#).

This section provides sample configuration information for Microsoft AD FS.

Follow this sequence of tasks to configure the Identity Provider.

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 64
2	Set Authentication Type. See Authentication Types, on page 65 .
3	Configure an Identity Provider (IdP), on page 63
4	Enable Signed SAML Assertions, on page 67
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 68

Sequence	Task
1	Install and Configure Active Directory Federation Services, on page 64
2	Set Authentication Type. See Authentication Types, on page 65 .
4	Enable Signed SAML Assertions, on page 67
5	Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID, on page 68

Install and Configure Active Directory Federation Services

Follow Microsoft instructions and guidelines to install Microsoft Active Directory Federation Services (AD FS).

For example, see *Active Directory Federation Services Overview* at [https://technet.microsoft.com/en-us/library/hh831502\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831502(v=ws.11).aspx)

- For AD FS in Windows Server (AD FS 3.0), see the *AD FS Content Map* at <http://aka.ms/adfscontentmap> and *AD FS Technical Reference* at [https://technet.microsoft.com/en-us/library/dn303410\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn303410(v=ws.11).aspx).
- For AD FS in Windows Server, see *AD FS Technical Reference* at <https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services>.



Note SSO for Unified CCE supports IdPs other than MS, and AD FS. For the list of supported IdPs see the Compatibility matrix <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html>



Note Cisco IdS does not support AD FS Automatic Certificate Rollover. If the AD FS certificate gets rolled over, then re-establish the trust relationship between the IdS and AD FS.



Note The Secure Hash Algorithm (SHA) used for signature verification between:

- IdP and Cisco IdS: SHA-1, SHA-256
- Cisco IdS and the application browsers: SHA-256

Authentication Types

Cisco Identity Service supports form-based authentication of the Identity Provider.

For information on enabling form-based authentication in ADFS, see Microsoft documentation:

- For ADFS 3.0 see <https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/>

For Kerberos authentication to work, ensure to disable the form-based authentication.

- In AD FS on Windows Server, set the Authentication Type to Forms-based authentication (FBA). Refer to the following Microsoft TechNet article, <http://social.technet.microsoft.com/wiki/contents/articles/1600.ad-fs-2-0-how-to-change-the-local-authentication-type.aspx>
- In AD FS on Windows Server, set the Authentication Policy to Forms Authentication. Refer to the following Microsoft TechNet article, <https://blogs.msdn.microsoft.com/josrod/2014/10/15/enabled-forms-based-authentication-in-adfs-3-0/>

In AD FS, be sure that the default Authentication Type is set to Forms.

Integrate Cisco IdS to the Shared Management AD FS

- Step 1** In AD FS, be sure that the default Authentication Type is set to Forms. (Cisco Identity Service requires the Identity Provider to provide form-based authentication.) See the Microsoft AD FS documentation for details.
- Step 2** In AD FS server, open **AD FS Management**.
- Step 3** Right-click **AD FS** -> **Trust Relationships** -> **Relying Party Trust**.
- Step 4** From the menu, choose **Add Relying Party Trust** to launch the **Add Relying Party Trust Wizard**.
- Step 5** In the **Select Data Source** step, choose the option **Import data about the relying party from a file**.
- Step 6** **Browse** to the `sp.xml` file that you downloaded from Cisco Identity Server and complete the import to establish the relying party trust.
- Step 7** Select the step **Specify Display Name**, and add a significant name you can use to identify the Relying Party Trust.
- Step 8** For AD FS in Windows Server, select the option **I do not want to configure multi-factor authentication settings for the relying party at this time** in the Step **Configure Multi-factor Authentication Now**.
- Step 9** In the Step Choose Issuance Authorization Rules, select the option **Permit all users to access this relying party** and click **Next**.
- Step 10** Click **Next** again to finish adding the relying party.
- Step 11** Right-click on the **Relying Party Trust** and click **Properties**. Select the **Identifiers** tab.
- Step 12** On the **Identifiers** tab, configure the following:

Field	Description
Display name	The unique name of the identifier.

Field	Description
Relying party identifier	FQDN of the publisher node of Cisco Identity Server from which you downloaded the Cisco IdS metadata file.
	FQDN of the subscriber node of Cisco Identity Server.

Step 13 Still in **Properties**, select the **Advanced** tab.

Step 14 Select **secure hash algorithm** as **SHA-1** and then click **OK**.

Note In the following steps, you configure two claim rules to specify the claims that are sent from AD FS to Cisco Identity Service as part of a successful SAML assertion:

- A claim rule with the following custom claims, as AttributeStatements, in the assertion:
 - **uid** - Identifies the authenticated user in the claim sent to the applications.
 - **user_principal** - Identifies the authentication realm of the user in the assertion sent to Cisco Identity Service.
- A second claim rule that is a NameID custom claim rule specifying the fully qualified domain name of the AD FS server and the Cisco IdS server.

Follow the steps to configure these rules.

Step 15 In **Relying Party Trusts**, right-click on the Relying Party Trust you created, and click **Edit Claim Rules**.

Step 16 Follow these steps to add a rule with **Send LDAP Attributes as Claims** as the Claim rule template.

- a) In the **Issuance Transform Rules** tab, click **Add Rule**.
- b) In the Step **Choose Rule Type**, select the claim rule template **Send LDAP Attributes as Claims** and click **Next**.
- c) In the **Configure Claim Rule** step, in the **Claim rule name** field, enter **NameID**.
- d) Set the **Attribute store** drop-down to **Active Directory**.
- e) Set the table **Mapping of LDAP attributes to outgoing claim types** to the appropriate **LDAP Attributes** and the corresponding **Outgoing Claim Type** for the type of user identifier you are using:
 - When the identifier is stored as a **SAM-Account-Name** attribute:
 1. Select an **LDAP Attribute** of **SAM-Account-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
 2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).
 - When the identifier is a UPN:
 1. Select an **LDAP Attribute** of **User-Principal-Name**, and set the corresponding **Outgoing Claim Type** to **uid** (lowercase).
 2. Select a second **LDAP Attribute** of **User-Principal-Name** and set the corresponding **Outgoing Claim Type** to **user_principal** (lowercase).

Note The SAM-Account-Name or UPN choice is based on the User ID configured in the AW.

- Step 17** Follow these steps to add a second rule with the template **custom claim rule**.
- Select **Add Rule** on the **Edit Claim Rules** window.
 - Select **Send Claims Using Custom Rule**.
 - Set the name of rule to the **fully qualified domain name (FQDN)** of the Cisco Identity Server publisher (primary) node.
 - Add the following rule text:


```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] =>
  issue (Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
    Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType,

    Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
      "urn:oasis:names:tc:SAML:2.0:nameid-format:transient",
    Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/namequalifier"] =
      "http://<AD FS Server FQDN>/adfs/services/trust",
    Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
      "<fully qualified domain name of Cisco Ids>");
```
 - Edit the script as follows:
 - Replace **<ADFS Server FQDN>** to match exactly (including case) the ADFS server FQDN (fully qualified domain name.)
 - Replace **<Cisco IdS server FQDN>** to match exactly (including case) the Cisco Identity Server FQDN.

- Step 18** Click **OK**.

Enable Signed SAML Assertions

Enable Signed SAML Assertions for the Relying Party Trust (Cisco Identity Service).

- Step 1** Click **Start** and type **powershell** in the Search field to display the Windows Powershell icon.
- Step 2** Right-click on the Windows Powershell program icon and select **Run as administrator**
- Note** All PowerShell commands in this procedure must be run in Administrator mode.
- Step 3** Run the command, **Set-ADFSRelyingPartyTrust -TargetName <Relying Party Trust Display Name> -SamlResponseSignature "MessageAndAssertion"**.
- Note** Set **<Relying Party Trust Display Name>** to exactly match (including case) the Identifier tab of the Relying Party Trust properties.
- For example:
- ```
Set-ADFSRelyingPartyTrust -TargetName CUICPub.PCCERCDN.cisco.com
-SamlResponseSignature "MessageAndAssertion".
```
- Step 4** Navigate back to the Cisco Identity Service Management window.
- Step 5** Click **Settings**.  
By default **IdS Trust** tab is displayed.
- Step 6** On the Download SAML SP Metadata and Upload IdP Metadata windows, click Next as you have already established trust relationship between IdP and IdS.

**Step 7** On the AD FS authentication window, provide the login credentials.

**Step 8** On successful SSO setup, the message "SSO Configuration is tested successfully" is displayed.

**Note** If you receive the error message "An error occurred", ensure that the claim you created on the AD FS is enabled.

If you receive the error message "IdP configuration error: SAML processing failed", ensure that the rule has the correct names for Ids and AD FS.

## Optionally Customize the AD FS Sign-In Page in Windows Server to Allow User ID

By default, the sign-in page presented to SSO users by AD FS in Windows Server requires a username that is a UPN. Usually this is an email format, for example, user@cisco.com. If your contact center solution is in a single domain, you can modify the sign-in page to allow your users to provide a simple User ID that does not include a domain name as part of the user name.

There are several methods you can use to customize the AD FS sign-in page. Look in the Microsoft AD FS in Windows Server documentation for details and procedures to configure alternate login IDs and customize the AD FS sign-in pages.

The following procedure is an example of one solution.

**Step 1** In the AD FS **Relying Party Trust**, change the NameID claim rule to map the chosen LDAP attribute to **uid**.

**Step 2** Click the Windows **Start** control and type **powershell** in the Search field to display the Windows Powershell icon.

**Step 3** Right-click on the Windows Powershell program icon and select **Run as administrator**

All PowerShell commands in this procedure must be run in Administrator mode.

**Step 4** To allow sign-ins to AD FS using the sAMAccountName, run the following Powershell command:

```
Set-AdfsClaimsProviderTrust -TargetIdentifier "AD AUTHORITY" -AlternateLoginID sAMAccountName
-LookupForests myDomain.com
```

In the LookupForests parameter, replace myDomain.com with the forest DNS that your users belong to.

**Step 5** Run the following commands to export a theme:

```
mkdir C:\themeExport-AdfsWebTheme -Name default -DirectoryPath c:\theme
```

**Step 6** Edit onload.js in C:\theme\script and add the following code at the bottom of the file. This code changes the theme so that the AD FS sign-in page does not require a domain name or an ampersand, "@", in the username.

```
// Update the placeholder text to not include the domain
var userNameInput = document.getElementById("userNameInput");
if (userNameInput) {
 userNameInput.setAttribute("placeholder", "Username");
}

// Override submitLoginRequest to not have the "@" check
Login.submitLoginRequest = function () {
 var u = new InputUtil();
 var e = new LoginErrors();
 var userName = document.getElementById(Login.userNameInput);
 var password = document.getElementById(Login.passwordInput);
 if (!userName.value) {
 u.setError(userName, e.userNameFormatError);
 }
}
```

```

 return false;
}
if (!password.value) {
 u.setError(password, e.passwordEmpty);
 return false;
}
document.forms['loginForm'].submit();
return false;
};

```

**Step 7** In Windows PowerShell, run the following commands to update the theme and make it active:

```

Set-AdfsWebTheme -TargetName custom -AdditionalFileResource
@{Uri='/adfs/portal/script/onload.js';path="c:\theme\script\onload.js"}

Set-AdfsWebConfig -ActiveThemeName custom

```

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

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

After the expiry of SHA-1, the administrator must configure SHA-256..

Perform this procedure after the upgrade has completed successfully.

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

**Step 2** Click **Settings**.

**Step 3** Click **Security** tab.

**Step 4** Click **Keys and Certificates**.

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

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

**Step 6** Download new metadata file. Click on **IdS Trust** tab and then click download button.

**Step 7** Change Secure Hash Algorithm in AD FS Relaying Party Trust configuration. In AD FS server, open AD FS Management. Go to **ADFS ->Trust Relationships->Relying Party Trusts**, right click on existing Relying Party Trust for Cisco IdS and then click on Properties. In the Advanced Tab, change the Secure Hash Algorithm to **SHA-256**. Click **Apply**.

**Step 8** Update Relying party trust on AD FS. From AD FS Server, run the following Powershell command:

```

Update-AdfsRelyingPartyTrust -MetadataFile <path to Step 6 new MetaData File> -TargetName
<Relying Party Trust Display Name>

```

## 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 72](#).

**Step 1** In the Unified CCE Administration, choose **Overview > Infrastructure Settings > Device Configuration > Identity Service**.

**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.



---

**Note** If SSO is enabled in the deployment, then import all the IdS server nodes certificate into Cisco Finesse, CUIIC, and LiveData component trust store.

---

## Register Components and Set Single Sign-On Mode

If you add any SSO-compatible machines to the System Inventory after you register components with the Cisco IdS, those machines are registered automatically.

### Before you begin

- Configure the Cisco Identity Service (Cisco IdS).
- Disable popup blockers. It enables viewing all test results correctly.

- 
- Step 1** In the Unified CCE Administration, navigate to **Features > Single Sign-OnOverview > Infrastructure Settings > Device Configuration > Identity Service**.
- Step 2** Click the **Register** button to register all SSO-compatible components with the Cisco IdS.  
The component status table displays the registration status of each component.  
If a component fails to register, correct the error and click **Retry**.
- Step 3** Click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when presented with a log in dialog, log in as a user with SSO credentials.  
The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.  
The component status table displays the status of testing each component.  
If a test is unsuccessful, correct the error, and then click **Test** again.  
Test results are not saved. If you refresh the page, run the test again before enabling SSO.
- Step 4** Select the SSO mode for the system from the **Set Mode** drop-down menu:
- Non-SSO: This mode disables SSO for all agents and supervisors. Users log in using existing Active Directory-based local authentication.
  - Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
  - SSO: This mode enables SSO for all agents and supervisors.
- The component status table displays the status of setting the SSO mode on each component.  
If the SSO mode fails to be set on a component, correct the error, and then select the mode again.
- 

## 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.

- 
- 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**.

---

## 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.

---



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

### Before you begin

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

**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: <ul style="list-style-type: none"> <li>• Unified CVP</li> <li>• Unified CVP Reporting</li> <li>• Virtualized Voice Browser</li> </ul>                                                                                                                                                                                    |
| Site         | Choose the site. You can run the REST API call on the Main site or the Remote site machines.<br>Default is All Sites when a Machine Type is selected.                                                                                                                                                                                                               |
| Host Name    | Choose a Host Name or multiple Host Names.<br>Host Names are displayed based on the selected Machine Type and Site.                                                                                                                                                                                                                                                 |
| Method       | Choose the HTTP method. Valid values are: <ul style="list-style-type: none"> <li>• GET</li> <li>• POST</li> <li>• PUT</li> <li>• DELETE</li> </ul> Default is GET.                                                                                                                                                                                                  |
| Path         | Enter the relative URI of the API.<br>Based on the Machine Type you select, most frequently used APIs are displayed as auto suggestions. For example, when the Machine Type is <b>Unified CVP</b> , the path displayed is <code>cvp-orm/rest/cvpconfig/properties</code> .<br>For more information about APIs, refer to the respective CCE Component documentation. |
| Request Body | Enter the request data in JSON or XML format.<br>Mandatory if the Method is POST or PUT.                                                                                                                                                                                                                                                                            |

| Field         | Description                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| Response Type | Choose the Response Type as JSON or XML. Default is JSON.<br><b>Note</b> Response Type is only applicable for Success result. |

**Step 3** Click **Execute**.

The window displays the Success or Failure response. You have an option to copy or export the success response. These options are available on the right side of the success response text area, only for GET method.

- Click **Copy** icon to copy the response text to a clipboard.
- Click **Export** icon to export the response text to a file. The file extension is based on the Response type. For example, if the Response Type is `xml`, the response is exported as `response.xml`.

**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 77
- [Add an Agent by Copying an Existing Agent Record](#), on page 82
- [Edit Description, Desk Settings, and Teams for Multiple Agents](#), on page 86
- [Enable or Disable Contact Center AI Services for Multiple Agents](#), on page 87
- [Add Supervisor Status to an Agent](#), on page 90
- [Attributes](#), on page 108
- [Desk Settings](#), on page 178
- [Roles](#), on page 91
- [Skill Groups](#), on page 105
- [Teams](#), on page 98

## 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 82](#)).
- Run bulk jobs to add or edit multiple agent records (see [Manage Bulk Jobs, on page 244](#)).
- Edit the skill group membership for multiple agents at once (see [Edit Skill Group Membership for Multiple Agents, on page 85](#)).
- Edit descriptions, desk settings, and teams for multiple agents at once (see [Edit Description, Desk Settings, and Teams for Multiple Agents, on page 86](#)).
- Edit Contact Center AI services for multiple agents at once (see [Enable or Disable Contact Center AI Services for Multiple Agents, on page 87](#)).

---

**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 Enable Digital Channels**, and **Contact Center AI** 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable SSO</b>    | no        | <p>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.</p> <p>You can check this check box to enable SSO for this agent if SSO is set globally to mixed mode.</p> <p>You cannot edit this setting if SSO is enabled or disabled globally.</p> <p>If SSO is enabled globally, saving the agent's new or updated record enables SSO for the agent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Login Enabled</b> | no        | Checked by default. Uncheck the check box only if you do not want this agent to be able to sign in.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Is Supervisor</b> | no        | <p>Check to configure this agent as a Supervisor.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• For an existing supervisor's record, if you uncheck this check box, the corresponding user account is deleted from Unified Intelligence Center.</li> </ul>                                                                                                                                                                                                                                                                                                                      |
| <b>Username</b>      | yes       | <p>Enter a unique username for the Agent.</p> <p>Enter up to 255 characters as the username. Supports all characters, except for the following:</p> <p>Double quotation mark ("), forward slash (/), backward slash (\), square brackets ([ ]), colon (:), semicolon (;), pipe ( ), equal to (=), comma (,), plus sign (+), asterisk (*), question mark (?), angle brackets (&lt;&gt;), and SPACE.</p> <p>For supervisors and for agents with single sign-on (SSO) enabled, the username is the user's Active Directory or SSO account username.</p> <p>For supervisors who are not enabled for single sign-on (SSO), the Active Directory username must be in the user@domain format.</p> <p><b>Remember</b> An agent who is designated as a supervisor signs in to Unified CCE Administration with this username.</p> <p><b>Note</b> Ensure that Agent ID (Peripheral number) and agent Login name is unique for each user.</p> |
| <b>First Name</b>    | yes       | See <a href="#">Character Sets</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Last Name</b>     | yes       | See <a href="#">Character Sets</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Field                 | Required?                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Agent ID</b>       | -                                     | <p>Enter a unique string of up to 11 digits.</p> <p>If you leave this field blank, Packaged CCE automatically generates a 7-digit agent ID, which you can later edit.</p> <p>The agent uses the Agent ID to sign in to Cisco Finesse.</p>                                                                                                                                                                                                                                                                                                                                                              |
| <b>Description</b>    | no                                    | <p>Enter a description of the agent.</p> <p>See <a href="#">Character Sets</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Desk Settings</b>  | -                                     | <p>The <b>Desk Settings</b> field defaults to show the current system-default. (See <a href="#">Main Site, on page 218</a>.) To change it, click the <b>magnifying glass</b> icon to display the <b>Select Desk Settings</b> list where you can select a different desk setting.</p>                                                                                                                                                                                                                                                                                                                   |
| <b>Department</b>     | yes (for departmental administrators) | <p>A departmental administrator must select one department from the pop-up list to associate with this agent. The list shows all administrator's departments.</p> <p>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.</p> <p>See <a href="#">Departments, on page 117</a> for more information about associating agents with departments.</p>                                                                                                                              |
| <b>Site</b>           | -                                     | <p>The <b>Site</b> field displays Main by default for Packaged CCE 2000 Agents deployment.</p> <p>For Packaged CCE 4000 Agents and 12000 Agents deployments, <b>Site</b> is a mandatory field and has no default value.</p> <p>To add a site:</p> <ol style="list-style-type: none"> <li>a. Click the <b>magnifying glass</b> icon to display the list of sites.</li> <li>b. Select the required site.</li> </ol>                                                                                                                                                                                      |
| <b>Peripheral Set</b> | yes                                   | <p>This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see <a href="#">Add and Maintain Peripheral Set</a>.</p> <p>To add a peripheral set:</p> <ol style="list-style-type: none"> <li>a. Click the <b>magnifying glass</b> icon to display the list of peripheral sets configured for the selected <b>Site</b>.</li> <li>b. Select the required peripheral set.</li> </ol>                                                                                                                                                                   |
| <b>Team</b>           | no                                    | <p>The <b>Team</b> field defaults to <i>None</i>. To change the setting, click the <b>magnifying glass</b> icon to display the <b>Select Team</b> list and select a team. Only the teams associated to the selected site display.</p> <p>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.</p> <p><b>Note</b> When you add a team to an agent, the same agent is added to the corresponding collection in the Unified Intelligence Center.</p> |

| Field                    | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Set Password</b>      | 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.<br><br>If single sign-on is enabled, the password settings on the <b>General</b> tab are disabled.                                                                                                                                                                                                                         |
| <b>Enter Password</b>    | no        | Enter and reenter a maximum of 256 ASCII characters to establish and confirm a password for this agent. Password is case-sensitive.<br><br>The default <i>Minimum Password Length</i> is set in system settings. (See <a href="#">Global</a> , on page 215.)<br><br>For a supervisor, the password must be the supervisor's Active Directory password.<br><br><b>Tip</b> An agent who is designated as a supervisor signs in to Unified CCE Administration with this password. |
| <b>Re-enter Password</b> | 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 Digital Channels** tab if Cloud Connect is added and registered or ECE is configured.

| Field                      | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Support Digital Channel    | No        | Check the check box to enable the agent for digital channel interaction.<br><br>This check box appears only if you have added Cloud Connect in your inventory and you have registered it in the Control Hub. For more information, see <a href="https://help.webex.com/en-us/article/n24wo0fb/Register-Cloud-Connect">https://help.webex.com/en-us/article/n24wo0fb/Register-Cloud-Connect</a> .                                                           |
| Support Email & Chat (ECE) | no        | This check box appears only when ECE is configured for a peripheral set or a data center. By default, it is not checked.                                                                                                                                                                                                                                                                                                                                   |
| 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.<br><br>This field is required if Support Email & Chat is checked. |

| Field         | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Email Address | no        | <p>The email address of the agent. Maximum length is 50 characters. Email address is mandatory when this checkbox is selected.</p> <p>The following must be true for any email address:</p> <ul style="list-style-type: none"> <li>• Must include only one @ character.</li> <li>• Must include at least one character between @ and dot ( . ).</li> <li>• Must include one dot ( . ) after @ character.</li> <li>• Dot ( . ) must not be the last character.</li> </ul> <p><b>Note</b> Characters like round bracket ( ), angular bracket &lt; &gt; , and double quote " should not be included in the email address.</p> |

**Step 8** Complete the **Contact Center AI** tab if Cloud Connect is added to the inventory and registered in the Control Hub. The tab displays the list of services (**Agent Answers**, **VAV Transcript**, and **Call Transcript**) for an agent and allows you to enable or disable the service.

- To enable a service, check the check box corresponding to the service.
- To disable a service, uncheck the check box corresponding to the service.

**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.

---

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

**Step 5** 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 85](#).




---

**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.

---

- 
- 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 different sites, departments, or peripheral sets.
- 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 83.](#))

**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 different sites, departments, or peripheral sets.
- 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 83.](#))

---

**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.

---

## Edit Attributes for Multiple Agents

In both Unified CCE and Packaged CCE deployments, the agents must all belong to the same site and same department, or all be global agents.

- The **Edit** button is disabled for a mix of global and departmental agents in Packaged CCE deployment.




---

**Note** 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 83](#))

---

### Before you begin

Using the Agent tool, you can edit attributes for multiple agents at once.

- 
- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Check the check box for each agent whose attribute 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 > Attribute**.
- The **# of Selected Agents** column indicates how many of the selected agents currently belong to each attribute.
- Step 4** In the **Action** column, click the **x** icon for each attribute from which you want to remove the selected agents.
- Note** If all selected agents belong to an attribute, the **x** icon along with the **dropdown** appears for that attribute. If none of the selected agents belong to an attribute, only the **dropdown** appears for that attribute.
- The total number of attributes that you are adding and removing appears at the bottom of the dialog.
- Step 5** To undo an attribute change, click the **Undo Update** icon in the **Action** column for that attribute.
- Step 6** Click **Save**, and then click **Yes** to confirm the changes.
- 

## Enable or Disable Contact Center AI Services for Multiple Agents

Administrators and supervisors can enable or disable Contact Center AI Services for multiple agents.

All agents must belong to the same site and the same department, or all agents must be global agents. The **Edit** button is disabled if:

- Agents from different sites, departments, or peripheral sets are selected.
- A mix of global and departmental agents are selected.

- 
- Step 1** In **Unified CCE Administration**, choose **Users > Agents**.
- Step 2** Check the check box corresponding to each agent whose services you want to edit.
- Step 3** Click **Edit > Contact Center AI**.  
The Edit Services dialog displays a list of services that are the service that is enabled or disabled.
- If the service is enabled for all the agents selected for editing, the check box is checked.
  - If the service is disabled for all the agents selected for editing, the check box is unchecked.
  - If the service is enabled for some agents and disabled for the others, the check box has a dash (—).
- Step 4** To enable or disable the Contact Center AI Services, check or uncheck the check boxes corresponding to the services.
- Step 5** Click **Save**, and then click **Yes** to confirm the changes.
- 

## Manage Security

The system generates agent passwords using advanced hashing.

Advanced hashing helps you to ensure greater security of agent passwords in non-SSO mode. To enforce advanced hashing of agent passwords, you must enable the **Enforce** button under the tab, **Manage Security**.

Before you enforce the global switch, consider the following to ensure that the agent authentication is successful.

1. All the PG's must be version 12.6 (1) or later.
2. All the agent passwords must be re-entered.

When you disable **Enforce**, the system authenticates passwords using old and advanced hashing. When you enable **Enforce**, the system authenticates passwords only using advanced hashing.




---

**Note** You will be able to disable the global switch from the API. For more information on how to disable the global switch see *Agent Security API* at <https://developer.cisco.com/docs/packaged-contact-center/#!agent-security-api-agent-security-api>

---




---

**Note** You will be able to disable the global switch from the API. For more information, on how to disable the global switch see *Agent Security API* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-programming-reference-guides-list.html>

---




---

**Note** The **Manage Security** option is removed from 12.6(1) ES34 onwards for Unified CCE deployments.

---

## 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 | <p>On the Agent List page, supervisors can see and edit settings for the agents that they supervise.</p> <ul style="list-style-type: none"> <li>• <b>General</b> tab: Supervisors can edit the password for agents who do not have single sign-on enabled. Other fields are read-only.</li> </ul> <p>After changing the agent's password,</p> <ul style="list-style-type: none"> <li>• The agent can sign in to Cisco Finesse only after 30 minutes, or</li> <li>• Restart Unified Intelligence Center Reporting Service and then the agent can sign in to Cisco Finesse.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Attributes</b> tab: Supervisors can add, modify, and remove attributes for agents on teams they supervise.</li> <li>• <b>Skill Groups</b> tab: Supervisors can add and remove the agent's membership in skill groups and can change the agent's default skill group.</li> <li>• <b>Supervised Teams</b> tab: Read-only for supervisors.</li> </ul> <p>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 <b>Edit &gt; Skill Groups</b> or <b>Edit &gt; Attributes</b>.</p> <p><b>Note</b> 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.</p> |

| Tool             | Permissions                                                                                                                                                                                                                                                                                                                                            |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Attributes       | On the Attributes List window, supervisors can see and edit agent attribute assignments. Supervisors cannot add or delete attributes. <ul style="list-style-type: none"> <li>• <b>General</b> tab: Fields are read-only.</li> <li>• <b>Agents</b> tab: Supervisors can add and remove attribute assignments for agents that they supervise.</li> </ul> |
| 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. <ul style="list-style-type: none"> <li>• <b>General</b> tab: Fields are read-only.</li> <li>• <b>Members</b> tab: Supervisors can add and remove skill groups for agents that they supervise.</li> </ul>        |
| 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**.

---

**Step 1** Create a new agent or edit an existing agent. See [Add and Maintain Agents, on page 77](#).

**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:

- Click **Add** next to **List of Supervised Teams** to open **Add Supervised Teams**.
- 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         | <p>The administrators assigned with this role can access the following features and subfeatures.</p> <ul style="list-style-type: none"> <li>• Agents: <ul style="list-style-type: none"> <li>• Manage Agents</li> <li>• Manage Agent Attributes</li> <li>• Reskill Agents</li> </ul> </li> <li>• Outbound Campaigns: <ul style="list-style-type: none"> <li>• Campaign Status &amp; Schedule</li> <li>• Campaign Contact</li> </ul> </li> <li>• Desktop Settings: <ul style="list-style-type: none"> <li>• Desktop Layout</li> <li>• Phonebook</li> <li>• Reason Codes</li> <li>• Workflow</li> </ul> </li> </ul> |

| Built-In Role Name | Associated Features and Subfeatures                                                                                                       |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| 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.

- 
- 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                                   | Yes       | Enter a unique name for the role, using a maximum of 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Description</b>                            | No        | Enter a maximum of 255 characters to describe the role.<br>See <a href="#">Character Sets</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Features and Subfeatures Access fields</b> | 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.<br><br><b>Note</b> 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.

**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. |

| Field                     | Required? | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                  | yes       | Enter a unique name for the administrator, using a maximum of 64 characters.<br><br>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 <a href="#">Character Sets</a> for details on valid characters for this field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Role                      | no        | <i>ConfigAdmin</i> is the default role for a new administrator. Click the <b>magnifying glass</b> icon to open the <b>List of Roles</b> pop-up window. Select a role for this administrator.<br><br>On the <b>Overview</b> page, the administrator can view only the cards and its access tools associated with the assigned role.<br><br>For more information see the topic                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Access to All Departments | no        | This check box defaults to checked. You cannot uncheck it for the <i>SystemAdmin</i> role—SystemAdmins are always Global administrators.<br><br>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: <ul style="list-style-type: none"> <li>• Click the + icon to open the <b>Add Departments</b> pop-up window.</li> <li>• 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.</li> <li>• Click the x icon to remove a department.</li> </ul> <p><b>Note</b> 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.</p> |

**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 97

[Administrators and System Access](#), on page 94

[Departments](#), on page 117

[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 117

## 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 16: 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 17: 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 18: Administrator Tools and Permissions**

| Administrator     | Tool        | Permissions                                                                                                                                                                                                                                                                            |
|-------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator One | Agent Tools | <ul style="list-style-type: none"> <li>• Full access to Agent Tools</li> <li>• View, add, edit, and delete Skill Group One</li> <li>• Add Admissions Department agents to Skill Group One</li> <li>• Add global agents to Skill Group One</li> <li>• View Skill Group Three</li> </ul> |
| Administrator Two | Agent Tools | <ul style="list-style-type: none"> <li>• Full access to Agent Tools</li> <li>• View, add, edit, and delete Skill Group Two</li> <li>• Add History Department agents to Skill Group Two</li> <li>• Add global agents to Skill Group Two</li> <li>• View Skill Group Three</li> </ul>    |



| Administrator       | Tool                  | Permissions                                                                                                                                                                                                              |
|---------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator Three | Script and Call Tools | <ul style="list-style-type: none"> <li>• Full access to Script and Call Tools</li> <li>• Full access to agents and Skill Groups from all departments</li> <li>• Full access to global agents and Skill Groups</li> </ul> |

## 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 administrator 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.

### Move to System Administrator Role

To add all the users in `ConfigAdmin` group to `UcceConfig` group:

1. Open **Computer Management > Local Users and Groups > Groups**.
2. Right click on **UcceConfig**, and select **Properties**.
3. Add all users with `ConfigAdmin` role into `UcceConfig` 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 76
- [Manage Supervisors](#), on page 88
- [Add and Maintain Desk Settings](#), on page 178

## Add and Maintain Teams

**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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Name</b>                          | Yes       | Enter up to 32 alphanumeric characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Description</b>                   | No        | Enter up to 255 characters to describe the team.<br>See <a href="#">Character Sets</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Site</b>                          | -         | The <b>Site</b> field displays Main by default for Packaged CCE 2000 Agents deployment type.<br><br>To add a different site:<br><b>a.</b> Click the <b>magnifying glass</b> icon to display the list of sites with Agent PG configured.<br><b>b.</b> Select the required site.                                                                                                                                                                                                                                          |
| <b>Peripheral Set</b>                | Yes       | <b>Note</b> Before you add a <b>Peripheral Set</b> , you must select a <b>Site</b> .<br><br>The <b>Peripheral Set</b> field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see <a href="#">Add and Maintain Peripheral Set</a> .<br><br>To select a peripheral set:<br><b>a.</b> Click the <b>magnifying glass</b> icon to display the list of peripheral sets that are configured for the selected <b>Site</b> .<br><b>b.</b> Select the applicable peripheral set. |
| <b>Supervisor DN (Dialed Number)</b> | No        | Click the <b>magnifying glass</b> icon to display the <b>Select Supervisor Script Dialed Number</b> list.<br><br>The list includes all dialed numbers with a routing type of <b>Internal Voice</b> .<br><br>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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Desktop Layout</b> | <p>To customize the site (and Peripheral Set available for Packaged CCE 4000 Agents and 12000 Agents deployments) specific desktop layout for the team:</p> <p>a. Check the <b>Customize</b> check box.</p> <p>You can now edit the <b>Desktop Layout</b> section. This section includes default desktop layout XML that is defined in <b>Desktop &gt; Resources &gt; Desktop Layout</b>.</p> <p>b. Select from the following editors:</p> <p><b>Note</b> To view the editors, install the ICM12.5(1)_ES07 patch.</p> <ul style="list-style-type: none"> <li>• Text Editor</li> <li>• XML Editor</li> </ul> <p>c. Edit the XML.</p> <p>To revert the changes, click <b>Revert Changes</b>.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• If you clear the <b>Customize</b> check box without saving the changes, the system reverts to the default desktop layout.</li> <li>• To add the Live Data report gadgets to the desktop layout, see <a href="#">Add Live Data Reports to Team Layout, on page 103</a>.</li> </ul> |

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Phone Books</b>       | <p>To assign phone books to the team:</p> <ol style="list-style-type: none"> <li>a. Click the + icon.<br/><br/>The <b>Add Phone Books</b> 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 <b>Teams in Desktop &gt; Resources</b>.</li> <li>b. Select one or more phone books from the list. Use the <a href="#">Sort a List</a> and <a href="#">Search a List</a> features to navigate the list.<br/><br/>The selected phone books are highlighted in the pop-up window, and appear in <b>List of Phone Books</b>. You can click the <b>Name</b> header to sort the phone books.</li> </ol> <p>To unassign a phone book from the team, click 'x' next to the phone book in <b>List of Phone Books</b>.</p>           |
| <b>Not Ready Reasons</b> | <p>To assign not ready reasons to the team:</p> <ol style="list-style-type: none"> <li>a. Click the + icon.<br/><br/>The <b>Add Not Ready Reasons</b> pop-up window opens with a list of not ready reasons. The reasons are configured as <b>Team Specific in Desktop &gt; Reason Labels &gt; Phone Books</b>.</li> <li>b. Select one or more reasons from the list. Use the <a href="#">Sort a List</a> and <a href="#">Search a List</a> features to navigate the list.<br/><br/><b>Note</b>        The search field does not allow searching the list by code.<br/><br/>The selected reasons are highlighted in the popup window, and appear in <b>List of Not Ready Reasons</b>. You can click the <b>Label</b> header to sort the reasons.</li> </ol> <p>To unassign a not ready reason from the team, click 'x' next to the reason in <b>List of Not Ready Reasons</b>.</p> |
| <b>Sign Out Reasons</b>  | <p>To assign sign out reasons to the team:</p> <ol style="list-style-type: none"> <li>a. Click the + icon.<br/><br/>The <b>Add Sign Out Reasons</b> popup window opens with a list of sign out reasons. The reasons are configured as <b>Team Specific in Desktop &gt; Reason Labels</b>.</li> <li>b. Select one or more reasons from the list. Use the <a href="#">Sort a List</a> and <a href="#">Search a List</a> features to navigate the list.<br/><br/><b>Note</b>        You cannot search the list by code in the pop-up window.<br/><br/>The selected reasons are highlighted in the pop-up window, and appear in <b>List of Sign Out Reasons</b>. You can click the <b>Label</b> header to sort the reasons.</li> </ol> <p>To unassign a sign out reason from the team, click 'x' next to the reason in <b>List of Sign Out Reasons</b>.</p>                           |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Wrap-Up Reasons</b> | <p>To assign wrap-up reasons to the team:</p> <ol style="list-style-type: none"> <li>Click the + icon.<br/>The <b>Add Wrap-Up Reasons</b> pop-up window opens with a list of wrap-up reasons. The reasons are configured as <b>Team Specific</b> in <b>Desktop &gt; Reason Labels</b>.</li> <li>Select one or more reasons from the list. Use the <a href="#">Sort a List</a> and <a href="#">Search a List</a> features to navigate the list.<br/>The selected reasons are highlighted in the popup window, and appear in <b>List of Wrap-Up Reasons</b>. You can click the <b>Label</b> header to sort the reasons.</li> </ol> <p>To unassign a wrap-up reason from the team, click 'x' next to the reason in <b>List of Wrap-Up Reasons</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Workflows</b>       | <p>To assign workflows to the team:</p> <ol style="list-style-type: none"> <li>Click the + icon.<br/>The <b>Add Workflow</b> pop-up window opens with a list of workflows that are configured for the site in <b>Desktop &gt; Resources &gt; Workflows</b>.</li> <li>Select one or more workflows from the list. Use the <a href="#">Sort a List</a> and <a href="#">Search a List</a> features to navigate the list.<br/><b>Note</b> You cannot search the list by description in the pop-up window.<br/>The selected workflows are highlighted in the pop-up window, and also appear in <b>List of Workflows</b>.</li> <li>Close the <b>Add Workflow</b> pop-up window.<br/>The workflows are carried out in the order they appear in the <b>List of Workflows</b>. The <b>Order</b> column displays the order of the workflow. The newly added workflow appears at the end of the list.</li> <li>To change the workflow order: <ol style="list-style-type: none"> <li>In the <b>Order</b> column, click the drop-down arrow that is associated with the workflow that you want to move.<br/>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.</li> <li>Select a number from the drop-down list.<br/>The workflow moves to the selected position in the <b>List of Workflows</b> table. The other workflows move a row up or down based on the new position of the workflow.</li> </ol> </li> </ol> <p>To unassign a workflow from the team, click 'x' next to the workflow in <b>List of Workflows</b>.</p> |

**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.

**Step 1** Sign in to the Finesse administration console.

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

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

**Step 4** Copy the XML code for the report you want to add from the Finesse default layout XML. If your agents use HTTP to access Finesse, copy the XML code for the HTTP report. If they use HTTPS, copy the XML code for the HTTPS report.

### Example:

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

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

**Step 5** Copy the XML code for the report you want to add from the Finesse default layout XML.

### Example:

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

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

**Step 6** Go to **Organization > Teams**, and open an existing team's record on the list window.

**Step 7** Click the **Team Resources** tab.

**Step 8** In the **Desktop Layout** tab, check the **Customize** check box.

**Step 9** Paste the XML within the tab tags where you want it to appear.

### Example:

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

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

```

 filterId_2=agent.id=CL%20teamName
 </gadget>
</tab>
<tab>
 <id>manageCall</id>
 <label>finesse.container.tabs.agent.manageCallLabel</label>
</tab>
</tabs>
</layout>

```

**Step 10** Replace my-cuic-server with the fully qualified domain name of your Cisco Unified Intelligence Center Server.

**Step 11** Optionally, change the gadget height.

**Example:**

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

```

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

```

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

**Step 12** Click **Save**.

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

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

**Note** You can also perform the above steps in Unified CCE Administration (<https://<Side A/B Unified CCE AW-HDS-DDS IP address>/cceedminnew>). 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 108

[Add and Maintain Skill Groups](#), on page 106

[Agents](#), on page 76

[Skill Groups or Precision Queues?](#), on page 111

[Manage Supervisors](#), on page 88

## Add and Maintain Skill Groups

**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
<b>Name</b>	yes	Enter a name using up to 32 alphanumeric characters.
<b>Description</b>	no	Enter up to 255 characters to describe the skill group. See <a href="#">Character Sets</a> .
<b>Site</b>	-	<p>The <b>Site</b> field displays Main by default for Packaged CCE 2000 Agents deployment type.</p> <p>To add a different site:</p> <ol style="list-style-type: none"> <li>Click the <b>magnifying glass</b> icon to display the list of sites with Agent PG configured.</li> <li>Select the required site.</li> </ol>
<b>Peripheral Set</b>	yes	<p><b>Note</b> Before you add a <b>Peripheral Set</b>, you must select a <b>Site</b>.</p> <p>The <b>Peripheral Set</b> field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see <a href="#">Add and Maintain Peripheral Set</a>.</p> <p>To select a peripheral set:</p> <ol style="list-style-type: none"> <li>Click the <b>magnifying glass</b> icon to display the list of peripheral sets configured for the selected <b>Site</b>.</li> <li>Select the applicable peripheral set.</li> </ol>
<b>Media Routing Domain</b>	no	<p>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 <i>Cisco_Voice</i>.</p> <p>To select a different Media Routing Domain:</p> <ol style="list-style-type: none"> <li>Click the <b>magnifying glass</b> icon to display <b>Select Media Routing Domain</b>.</li> <li>Click a row to make a selection and close the list.</li> </ol>

Field	Required	Description
<b>Bucket Interval</b>	no	<p>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 <a href="#">Global, on page 215</a>.</p> <p>To select a different bucket interval:</p> <ol style="list-style-type: none"> <li><b>a.</b> Click the <b>magnifying glass</b> icon to display <b>Select Bucket Intervals</b>.</li> <li><b>b.</b> Click a row to make a selection and close the list.</li> </ol> <p>Click the <b>x</b> icon to clear the selection.</p>
<b>Service Level Threshold</b>	no	<p>Enter a value in seconds that you set as a goal for connecting a call with an agent.</p> <p>The field defaults to the threshold configured for this Media Routing Domain.</p> <p>Leave this field blank to use the service level threshold value for the Media Routing Domain.</p> <p>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.</p>
<b>Service Level Type</b>	no	<p>Select a service level type.</p> <p>Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation.</p> <ul style="list-style-type: none"> <li>• <b>Use Media Routing Domain Value</b> (the default): Select this option to use the value that is currently defined for the MRD.</li> <li>• <b>Ignore Abandoned Calls:</b> Select this option if you want abandoned calls to be excluded from the service level calculation.</li> <li>• <b>Abandoned Calls have Negative Impact:</b> 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.</li> <li>• <b>Abandoned Calls have Positive Impact:</b> 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.</li> </ul>

**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 109

[Precision Queues](#), on page 109

## Add and Maintain Attributes

- 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
<b>Name</b>	yes	Type a unique attribute name. For example, to create an attribute for mortgage insurance, type <i>mortgage</i> .
<b>Description</b>	no	Enter a maximum of 255 characters to describe the attribute. See <a href="#">Character Sets</a> .
<b>Type</b>	no	Select the type: Boolean or Proficiency.
<b>Default</b>	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.

Steps	
Name	Criteria
Step 1	[ (Spanish == 10) and (Boston == true) ] OR [ (ServerXYZ >= 6) and (Spanish >= 6) ]

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 109](#)).

### SUMMARY STEPS

1. Navigate to **Unified CCE Administration > Organization > Skills > Precision Queues**.
2. Click **New** to open the **New Precision Queue** window. Complete the fields.
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.
4. When you have finished adding, click **Save**.

### DETAILED STEPS

**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 <a href="#">Character Sets</a> .
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 <i>Cisco_Voice</i> .  To select a different Media Routing Domain: <ol style="list-style-type: none"> <li>a. Click the <b>magnifying glass</b> icon to display <b>Select Media Routing Domain</b>.</li> <li>b. Click a row to make a selection and close the list.</li> </ol>



Name	Required?	Description
<b>Service Level Type</b>	yes	<p>Select the service level type used for reporting on your service level agreement.</p> <p>Service level type indicates how calls that are abandoned before the service level threshold affect the service level calculation.</p> <ul style="list-style-type: none"> <li>• <b>Ignore Abandoned Calls</b> (the default): Select this option if you want to exclude abandoned calls from the service level calculation.</li> <li>• <b>Abandoned Calls have Negative Impact:</b> 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.</li> <li>• <b>Abandoned Calls have Positive Impact:</b> 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.</li> </ul>
<b>Service Level Threshold</b>	yes	<p>Enter the time in seconds that calls are to be answered based on your service level agreement, from 0 to 2,147,483,647.</p> <p>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.</p>

Name	Required?	Description
<b>Agent Order</b>	yes	<p>Select an option to determine which agents receive calls from this queue.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Longest Available Agent</b> (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.</li> <li>• <b>Most Skilled Agent</b>: 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.</li> <li>• <b>Least Skilled Agent</b>: The call is delivered to the agent who has the lowest competency sum from all the attributes pertinent to the Precision Queue step.</li> </ul>
<b>Bucket Intervals</b>	no	<p>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 <a href="#">Global</a>, on page 215).</p> <p>To select a different bucket interval:</p> <ol style="list-style-type: none"> <li>a. Click the <b>magnifying glass</b> icon to display <b>Select Bucket Intervals</b>.</li> <li>b. Click a row to make a selection and close the list.</li> </ol>

**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.

**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.

The screenshot shows a 'Step 1' configuration window with a close button (X) in the top right corner. At the top, there is a 'Wait for' field with a placeholder and the unit 'seconds'. Below this, there are two expression panels. The first panel, 'Expression 1', has a green 'Add Attribute' button with a dropdown arrow. It contains two rows: the first row has 'Spanish' in a searchable field, a '>=' operator dropdown, and a '8' value dropdown with a red 'X' delete icon; the second row has an 'AND' operator dropdown, 'ServerXYZ' in a searchable field, a '>=' operator dropdown, and an '8' value dropdown with a red 'X' delete icon. The second panel, 'Expression 2', has an 'OR' operator dropdown and a green 'Add Attribute' button with a dropdown arrow. It contains two rows: the first row has 'NewEngland' in a searchable field, an '==' operator dropdown, and a 'True' value dropdown with a red 'X' delete icon; the second row has an 'OR' operator dropdown, 'Boston' in a searchable field, an '==' operator dropdown, and a 'True' value dropdown with a red 'X' delete icon. At the bottom of the window are 'OK' and 'Cancel' buttons. A small vertical number '510290' is visible on the right side of the window.

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 116](#) 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 proficiency 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 create 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 19: 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 20: Rules for Relationships Between Teams and Agents and Teams and Supervisors**

	Agent - Global	Agent - Departmental	Supervisor - Global	Supervisor - Departmental
<b>Team - Global</b>	yes	yes	yes	no
<b>Team - Departmental</b>	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 93](#).

### 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](#).

- 
- 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:
- Name** (Required) Enter a unique name for the department, using a maximum of 32 characters.  
**Important** Do not name the department as `Service` or `Global`.
  - 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.
- Click the + icon to open the **Add Administrators** popup window.
  - Click one or more rows to select administrators; then close the popup window. The administrators are now on the List of Administrators.
  - 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](#).

**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
<b>Name</b>	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.  <b>Note</b> You cannot use the system reserved terms such as <b>dnc</b> and <b>none</b> as a campaign name.
<b>Status</b>	-	The option to enable or disable the campaign. It is enabled by default.
<b>Type</b>	-	Displays <b>Agent Based</b> by default.
<b>Dialing Mode</b>	Yes	Select a dialing mode from the drop-down list. <ul style="list-style-type: none"> <li>• <b>Predictive</b>: 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.</li> <li>• <b>Progressive</b>: 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.</li> <li>• <b>Preview</b>: The agent previews customer information on their desktop, and chooses to contact the customer, skip to another customer, or reject the call.</li> <li>• <b>Preview Direct</b>: This is similar to the Preview mode, except that the dialer automatically dials the call from the agent's phone after the agent accepts.</li> </ul>
<b>Description</b>	No	Enter up to 255 characters to describe the campaign.  See <a href="#">Character Sets</a> .

Field	Required?	Description
<b>Department</b>	Yes (for department administrators only)	A departmental administrator must select one department from the department popup list to associate with this campaign. The list shows all of this administrator's departments. (See <a href="#">Departments, on page 117.</a> )  A global administrator can leave this field set to default, which establishes the campaign as global (belonging to no departments). A global administrator can also select a department for this campaign.
<b>Schedule section</b>		
<b>Start Date</b>	No	The date that the campaign starts.
<b>End Date</b>	No	The date that the campaign ends.
<b>Start Time</b>	Yes	The time the campaign starts dialing customer numbers.
<b>End Time</b>	Yes	The time the campaign stops dialing customer numbers.
<b>Time Zone</b>	Yes	The time zone where the campaign runs.
<b>Dialing Option section</b>		
<b>Note</b>	This section appears only after you select the <b>Dialing Mode</b> as <b>Predictive</b> or <b>Progressive</b> .	
<b>Lines Per Agent</b>	No	The number of lines dedicated to each agent in the campaign. Range is 1 – 100. Default is 1.5.
<b>Maximum Lines Per Agent</b>	No	This field appears only after you select the <b>Dialing Mode</b> as <b>Predictive</b> .  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.
<b>Call Abandon Limit</b>	-	This field appears only after you select the <b>Dialing Mode</b> as <b>Predictive</b> .  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.
<b>Limit</b>	No	You can set the limit for abandon calls only after you enable the <b>Call Abandon Limit</b> option.  You can set a limit (0.1-100) for the percentage of abandoned calls in a campaign.  If the <b>Call Abandon Limit</b> option is disabled, the campaign dials without regard to the abandon limit.
<b>Call Progress Analysis (CPA)</b>	-	Enabled by default.  <b>Note</b> If you keep it enabled, make sure you have configured and enabled Call Progress Analysis in the Voice Gateway.

Field	Required?	Description
<b>Record CPA</b>	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files.
<b>Answering Machine Treatment</b>	-	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: <ul style="list-style-type: none"> <li>• <b>Abandon Call:</b> Drops the call, marks it as an answering machine, and schedules a retry. This option is selected by default.</li> <li>• <b>Transfer to Agent:</b> Transfers the call to an agent.</li> <li>• <b>Transfer to IVR Route Point:</b> Transfers the call to play a prerecorded message. The IVR route point is configured in the <b>Skill Group selection</b> dialog box on the <b>Skill Groups</b> tab.</li> </ul>
<b>Terminate Tone Detect</b>	-	This field is activated only when the <b>Answering Machine Treatment</b> field enabled and you select the <b>Transfer to IVR Route Point</b> 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.
<b>Callback Settings</b> section		
<b>Personalized Callback</b>	-	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.
<b>Missed Callback</b>	Yes (When <b>Personalized Callback</b> option is enabled.)	Select an option from the drop-down list to handle the personal callback in case the agent is not available. <ul style="list-style-type: none"> <li>• <b>Abandon:</b> Abandon the personal callback. This option is selected by default.</li> <li>• <b>Same time next business day:</b> Reschedule the personal callback to the same time the next business day.</li> <li>• <b>Use campaign dialed number:</b> Use the alternate dialed number.</li> </ul>

**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
<b>Site</b>	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
<b>Peripheral Set</b>	Yes	<p>This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see <a href="#">Add and Maintain Peripheral Set</a>.</p> <p>Select a peripheral set from the drop-down list. The list contains the peripheral sets associated to the selected site.</p>
<b>Skill Group</b>	Yes	<p>Click the <b>Search</b> icon to open the <b>Add a Skill Group</b> pop-up.</p> <p>You can search and select the Skill Group based on the name and description.</p> <p>The search result does not display the Skill Groups that are already added to a Campaign.</p>
<b>Dialed Number</b>	Yes	<p>Click the <b>Search</b> icon to open the <b>Add Dialed Number</b> pop-up.</p> <p>By default, you can view all the dialed numbers for which the <b>Routing Type</b> is set as <b>Outbound Voice</b>.</p> <p>You can search and select the dialed number based on the string value and description.</p> <p>The search result does not display the dialed numbers that are already added to a Campaign.</p> <p>The selected number is dialed to reserve an agent in the configured skill group.</p>
<b>Contact Records Cache Size</b>	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.
<b>Reserve Additional Agents</b>	No	<p>This field is available only if the dialing mode is selected as <b>Preview</b> or <b>Preview Direct</b> on the <b>General</b> tab.</p> <p>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.</p>
<b>Dialed Numbers for Transferring to an IVR Section</b>		
<b>Answering machine to IVR</b>	No	<p>Click the <b>Search</b> icon to open the <b>Add Dialed Number</b> pop-up.</p> <p>By default, you can view all the dialed numbers for which the <b>Routing Type</b> is set as <b>Outbound Voice</b>.</p> <p>You can search and select the dialed number based on the string value and description.</p> <p>The selected number indicates the route point required to do the transfer to IVR routing script.</p>

Field	Required?	Description
<b>Agent not available for IVR</b>	No	<p>Click the <b>Search</b> icon to open the <b>Add Dialed Number</b> pop-up.</p> <p>By default, you can view all the dialed numbers for which the <b>Routing Type</b> is set as <b>Outbound Voice</b>.</p> <p>You can search and select the dialed number based on the string value and description.</p> <p>The selected number is dialed to play a message to the calls about to be disconnected due to lack of available agents.</p>

**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
<b>Dialing Option</b> section		
<b>No answering ring limit</b>	No	Enter the number of times the system allows a dialed phone number to ring. Range is 2 – 10. Default is 4.
<b>Maximum attempts</b>	No	Enter the maximum number of attempts, including callbacks and retries. Range is 1 – 100. Default is 3.
<b>Abandoned call wait time</b>	Yes	<p>Enter the minimum duration (in seconds) of an outbound call. Range is 0 – 10. Default is 1.</p> <p><b>Note</b> 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.</p>
<b>Campaign prefix digits</b>	No	Enter the digits to prefix to each customer number dialed from this campaign. Maximum length is 15 digits.
<b>Retries</b> section		
<b>No answer delay</b>	No	Enter the time (in minutes) the dialer waits before calling back a no-answer call. Range is 1 – 99999. Default is 60.
<b>Busy signal delay</b>	No	Enter the time (in minutes) the dialer waits before calling back a busy phone number. Range is 1 – 99999. Default is 60.
<b>Customer abandoned delay</b>	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.

Field	Required?	Description
<b>Dialer abandoned delay</b>	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.
<b>Answering machine delay</b>	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.
<b>Customer not home delay</b>	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.
<b>Call Progress Analysis(CPA) Parameters</b> section		
<b>Minimum Silence Period(100-1000)</b>	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.
<b>Analysis Period(1000-10000)</b>	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.
<b>Minimum Valid Speech(50-500)</b>	NO	Minimum number of milliseconds of voice required to qualify a call as voice detected. Default is 112.
<b>Maximum Analysis Time(1000-10000)</b>	NO	Maximum number of milliseconds allowed for analysis before identifying a problem analysis as dead air/low volume. Default is 3000.
<b>Maximum termination tone analysis(1000-60000)</b>	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](#).

**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
<b>Name</b>	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.  <b>Note</b> You cannot use the system reserved terms such as <b>dnc</b> and <b>none</b> as a campaign name.
<b>Status</b>	-	The option to enable or disable the campaign. It is enabled by default.
<b>Type</b>	-	The default field value is set to <b>IVR Based</b> . You cannot edit this field.
<b>Dialing Mode</b>	Yes	From the drop-down list, choose the dialer type for the current IVR campaign.  <ul style="list-style-type: none"> <li>• <b>Predictive</b>: The dialer component determines the number of customers to dial per IVR port, based on the abandoned rate.</li> <li>• <b>Progressive</b>: The administrator specifies a fixed number of lines to dial per IVR port.</li> </ul> <b>Note</b> 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.
<b>Description</b>	No	Enter a description about the campaign using up to 255 characters.  See <a href="#">Character Sets</a> .
<b>Department</b>	Yes (for department administrators only)	A departmental administrator must select one department from the department popup list to associate with this campaign. The list shows all of this administrator's departments. (See <a href="#">Departments, on page 117</a> .)  A global administrator can leave this field set to default, which establishes the campaign as global (belonging to no departments). A global administrator can also select a department for this campaign.
<b>Schedule section</b>		
<b>Start Date</b>	No	Select the date that the campaign starts.
<b>End Date</b>	No	Select the date that the campaign ends.
<b>Start Time</b>	Yes	Enter the time that the campaign starts dialing the customer numbers.
<b>End Time</b>	Yes	Enter the time that the campaign stops dialing the customer numbers.
<b>Time Zone</b>	Yes	Choose the time zone where the campaign runs.
<b>Dialing Option section</b>		
<b>Lines Per Agent</b>	No	The number of lines dedicated to each IVR port for the campaign. Range is 1 – 100. Default is 1.5.

Field	Required?	Description
<b>Maximum Lines Per Agent</b>	No	This field appears only after you select the <b>Dialing Mode</b> as <b>Predictive</b> . 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.
<b>Abandon Calls Limit</b>	-	This field appears only after you select the <b>Dialing Mode</b> as <b>Predictive</b> .  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.
<b>Limit</b>	No	You can set the limit for abandon calls only after you enable the <b>Call Abandon Limit</b> option.  You can set a limit (0.1-100) for the percentage of abandoned calls in a campaign.  If the <b>Call Abandon Limit</b> option is disabled, the campaign dials without regard to the abandon limit.
<b>Call Progress Analysis (CPA)</b>	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files.  <b>Note</b> If you keep it enabled, make sure you have configured and enabled Call Progress Analysis in the Voice Gateway.
<b>Record CPA</b>	-	If you enable this option, the gateway provides a media stream and the dialer records the .wav files.
<b>Answering Machine Treatment</b>	-	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: <ul style="list-style-type: none"> <li>• <b>Abandon Call</b>: Drops the call, marks it as an answering machine, and schedules a retry. This option is selected by default.</li> <li>• <b>Transfer to IVR Route Point</b>: Transfers the call to play a prerecorded message. The IVR route point is configured in the <b>Skill Group selection</b> dialog box on the <b>Campaign Skill Groups</b> tab.</li> </ul> <b>Note</b> After you configure a Transfer to IVR Route Point, you cannot set the AMD records as <b>Retry</b> . Use a customized query to identify such calls and create a new campaign.
<b>Terminate Tone Detect</b>	-	This field is activated only when the <b>Answering Machine Treatment</b> field enabled and you select the <b>Transfer to IVR Route Point</b> 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.
<b>Callback Settings</b> section		



Field	Required?	Description
<b>Personalized Callback</b>	-	Enable this option allows the IVR port to schedule a callback to a customer for a specific date and time.
<b>Missed Callback</b>	Yes (When <b>Personalized Callback</b> option is enabled.)	Select an option from the drop-down list to handle the personal callback in case the agent is not available. <ul style="list-style-type: none"> <li>• <b>Abandon</b>: Abandon the callback. This option is selected by default.</li> <li>• <b>Same time next business day</b>: Reschedule the callback to the same time the next business day.</li> <li>• <b>Use campaign dialed number</b>: Use the alternate dialed number.</li> </ul>

**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
<b>Site</b>	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.
<b>Peripheral Set</b>	Yes	This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see <a href="#">Add and Maintain Peripheral Set</a> . Select a peripheral set from the drop-down list. The list contains the peripheral sets associated to the selected site.
<b>Skill Group</b>	Yes	Click the <b>Search</b> icon to open the <b>Add a Skill Group</b> 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.
<b>Dialed Number</b>	Yes	Click the <b>Search</b> icon to open the <b>Add Dialed Number</b> pop-up. By default, you can view all the dialed numbers for which the <b>Routing Type</b> is set as <b>Outbound Voice</b> . 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.
<b>Contact Records cache Size</b>	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.

Field	Required?	Description
<b>Number of IVR Ports</b>	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.
<b>Dialed Numbers for Transferring to an IVR Section</b>		
<b>Answering Machine to IVR</b>	Yes	Click the <b>Search</b> icon to open the <b>Add Dialed Number</b> pop-up.  By default, you can view all the dialed numbers for which the <b>Routing Type</b> is set as <b>Outbound Voice</b> .  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
<b>Dialing Option</b> section		
<b>No answering ring limit</b>	No	Enter the number of times the system allows a dialed phone number to ring. Range is 2 – 10. Default is 4.
<b>Maximum attempts</b>	No	Enter the maximum number of attempts, including callbacks and retries. Range is 1 – 100. Default is 3.
<b>Abandoned call wait time</b>	Yes	Enter the minimum duration (in seconds) of an outbound call. Range is 0 – 10. Default is 1.  <b>Note</b> 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.
<b>Campaign prefix digits</b>	No	Enter the digits to prefix to each customer number dialed from this campaign. Maximum length is 15 digits.

Field	Required?	Description
<b>Retries section</b>		
<b>No answer delay</b>	No	Enter the time (in minutes) the dialer waits before calling back a no-answer call. Range is 1 – 99999. Default is 60.
<b>Busy signal delay</b>	No	Enter the time (in minutes) the dialer waits before calling back a busy phone number. Range is 1 – 99999. Default is 60.
<b>Customer abandoned delay</b>	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.
<b>Dialer abandoned delay</b>	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.
<b>Call Progress Analysis(CPA) Parameters section</b>		
<b>Minimum Silence Period(100-1000)</b>	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.
<b>Analysis Period(1000-10000)</b>	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.
<b>Minimum Valid Speech(50-500)</b>	NO	Minimum number of milliseconds of voice required to qualify a call as voice detected. Default is 112.
<b>Maximum Analysis Time(1000-10000)</b>	NO	Maximum number of milliseconds allowed for analysis before identifying a problem analysis as dead air/low volume. Default is 3000.
<b>Maximum termination tone analysis(1000-60000)</b>	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.

**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.

**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.

- 
- 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

**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
<b>Status</b>	-	Select one of the following statuses for the business hour: <ul style="list-style-type: none"> <li>• <b>Open/Closed as per Business Calendar</b></li> <li>• <b>Force Open</b></li> <li>• <b>Force Close</b></li> </ul>
<b>Status Reason</b>	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.
<b>Name</b>	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.
<b>Description</b>	No	Enter a description of the business hour.
<b>Time Zone</b>	Yes	Select a time zone of the business hour from the drop-down list.
<b>Department</b>	-	Search and select a department to associate with the business hour. Default is Global. <p><b>Note</b> This is applicable for Packaged CCE deployment only.</p>

**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
<b>Date</b>	Yes	Select a date from the calendar.
<b>Description</b>	No	Enter a description for the special hour.
<b>Status</b>	-	Select a status. If the status is <b>Open</b> , the <b>Start Time</b> and <b>End Time</b> fields are enabled.
<b>Start Time</b>	Yes, if status is Open.	Select a start time for the special hour.
<b>End Time</b>	Yes, if status is Open.	Select an end time for the special hour.
<b>Duration</b>	-	Displays the duration of the special hour.
<b>Status Reason</b>	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.

- Click **Import** to open the **Import Special Hours and Holidays** pop-up window.
- Click the download icon to download the Special Hours & Holidays template. Use this template to enter the special hours and holidays.
- 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.

**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.

---

- 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.

---

- 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 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 at least 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.

### Edit Call Variables

Administrator can set call variables (callVariable1 to callVariable10) values and ECC variable values as editable. Amongst BA (campaign-based outbound calls) variables, only BAResponse can be edited. The agent and the supervisor can edit the call variable values during an active call or in the wrap-up state.



- 
- Note**
- Cisco Finesse refers to the ECC variable length from the AWDB and this length is validated while you edit the ECC variable. Cisco Finesse server takes about 15 minutes to update these changes from AWDB. Agents must sign in again for the ECC variable configuration changes to reflect in the Cisco Finesse desktop.
  - Call variables edit operation updates the values of the variables within the particular call. All entities listening to dialog events receive the updated call variables through the Cisco Finesse notifications. If any CTI clients are connected to the same Agent PG, they also receive notifications of the changed call data though CTI call events. However, application scripts or databases that are used to populate the call variables are not directly affected by this edit.
-



**Note** Call variables edit operation updates the values of the variables within the particular call. All entities listening to dialog events receive the updated call variables through the Cisco Finesse notifications. If any CTI clients are connected to the same Agent PG, they also receive notifications of the changed call data though CTI call events. However, application scripts or databases that are used to populate the call variables are not directly affected by this edit.

For more information on call variable limits, see the *Solution Design Guide for Cisco Unified Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html>.

For more information on call variable limits, see the *Solution Design Guide for Cisco Packaged Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/products-technical-reference-list.html>.

## Configure Call Variables Layouts

- 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.

## Add ECC Variables to Call Variables Layout

**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** Turn on the toggle switch to enable the edit option for a specific call variable. By default, this option is turned off.

**Note**

- Call variable (callVariable1 to callVariable10) values are editable.
- ECC variable values are editable.
- Amongst BA variables (campaign-based outbound calls), only BAResponse value is editable.

**Step 7** 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 8** To view the latest configured Call Variables Layout, click **Refresh** from the Call Variables Layouts gadget.

## Add ECC Variables to Call Variables Layout

**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

**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
- 

### 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 142](#).

Actions on the **Desktop Layouts** gadget are as follows:

- Edit the code using any of the following editors:
  - **Text Editor**
  - **XML Editor**
- **View Default Layout** - Displays the Cisco Finesse default layout.
- **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.

---

- Step 1** Sign in to the Finesse administration console.
- Step 2** Click the **Desktop Layout** tab.
- Step 3** Click **Finesse Default Layout XML** to show the default layout XML.
- Step 4** Copy the gadget URL for the report you want to modify from the Finesse default layout XML and paste it into a text editor.

**Example:**

If you want to modify the Agent Report for HTTPS, copy the following URL and paste it into a text editor:

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

- Step 5** In Cisco Unified Intelligence Center, in Edit view of the report, select the view for which you want to create a gadget URL and then click **Links**.
- The HTML Link field displays the permalink of the customized report.
- Step 6** Copy the permalink of the customized report from the **HTML Link** field, and paste it in a text editor. Then copy the viewId value from this link into the desired view.

**Example:**

Copy the viewId, which is underlined in this example, from the permalink for the report.

```
https://<Server Name>:8444/cuic/permalink/PermalinkViewer.htmx?
viewId=5C90012F10000140000000830A4E5B33&linkType=htmlType&viewType=Grid
```

- Step 7** Replace the desired viewId value in the gadget URL with the viewId value from the permalink of the customized report.
- Step 8** Replace my-cuic-server with the FQDN of the Cisco Unified Intelligence Center Server.
- Step 9** Add the customized gadget URL to the desktop layout XML in the Manage Desktop Layout gadget and click **Save**.

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

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

## 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.

**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 **Desktop Layouts** supports the following types of editors:

- **Text Editor**—A plain text editor. It is the default editor. You can use the **Expand All** option to see all the code details and Search text box to refine your search results.
- **XML Editor**—An XML editor.



- Note**
- You cannot add or edit comments (<!-- and -->) in the **XML Editor**.
  - In this document, all the examples that are related to desktop layout are applicable for text editor.

Both the editors support the following features:



- Expand and collapse option.
- Syntax highlights and color code for the visual indication.
- Auto-complete suggestions and hints for valid elements in the tags.

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:

- Sample configurations for customizing desktop properties are added to the default layout (**Desktop Layout**) and team-specific layout (**Team Resources > Desktop Layout**).

For upgraded layouts, sample configurations for customizing desktop properties do not appear by default. The administrator must copy the XML from the **View Default Layout** and add to the respective custom layouts.

- 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, the changes you make take effect on the desktop after 3 seconds. However, agents who are signed in when the changes are made must sign out and sign in again to see those changes reflect 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 141](#).

### Step 1 Click Desktop Layout.

**Step 2** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 3** 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>https://<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>
```

**Step 4** 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 5** 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.

The Finesse default XML layout is as follows:

```
<finesseLayout xmlns="http://www.cisco.com/vtg/finesse">
 <!-- DO NOT EDIT. The version number for the layout XML. -->
 <version>1250.03</version>
 <configs>
 <!-- The Title for the application which can be customized. -->
 <config key="title" value="Cisco Finesse"/>
 <!-- The following entries are examples of changing defaults for desktop properties.

 To change any property, uncomment the respective line and set the appropriate value.

 For more details on the properties that can be customized, refer to the Cisco Finesse
 Administration Guide.
 Note: The customized properties can only be set in the configs section and are not
 role-specific. -->
 <!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
 <!-- <config key="wrapUpCountDown" value="true"/> -->
 <!-- <config key="desktopChatAttachmentEnabled" value="true"/> -->
 <!-- <config key="forceWrapUp" value="true"/> -->
 <!-- Possible Values: supervisor_only, conference_controller_and_supervisor, all
-->
 <!-- <config key="enableDropParticipantFor" value="supervisor_only"/> -->
 <!-- Possible Values: agents, all -->
 <!-- <config key="dropParticipant" value="agents"/> -->
 <!-- The logo file for the application -->
 <!-- For detailed instructions on using custom icons for logos and tabs,
 please refer to the section "Customize Title and Logo in the Header"
 in the Finesse Administration Guide. -->
 <!-- <config key="logo" value="/3rdpartygadget/files/cisco_finext_logo.png"/> -->
 </configs>
 <header>
 <!-- Please ensure that at least one gadget/component is present within every
headercolumn tag -->
 <leftAlignedColumns>
 <headercolumn width="300px">
 <component id="cd-logo">
 <url>/desktop/scripts/js/logo.js</url>
 </component>
 </headercolumn>
 <headercolumn width="230px">
 <component id="agent-voice-state">
```

```

 <url>/desktop/scripts/js/agentvoicestate.component.js</url>
 </component>
</headercolumn>
<headercolumn width="251px">
 <component id="nonvoice-state-menu">
 <url>/desktop/scripts/js/nonvoice-state-menu.component.js</url>
 </component>
</headercolumn>

</leftAlignedColumns>
<rightAlignedColumns>
 <headercolumn width="50px">
 <component id="broadcastmessagepopover">
 <url>/desktop/scripts/js/teammessage.component.js</url>
 </component>
 </headercolumn>
 <headercolumn width="50px">
 <component id="chat">
 <url>/desktop/scripts/js/chat.component.js</url>
 </component>
 </headercolumn>
 <headercolumn width="50px">
 <component id="make-new-call-component">
 <url>/desktop/scripts/js/makenewcall.component.js</url>
 </component>
 </headercolumn>
 <headercolumn width="72px">
 <component id="identity-component">
 <url>/desktop/scripts/js/identity-component.js</url>
 </component>
 </headercolumn>
</rightAlignedColumns>
</header>
<layout>
 <role>Agent</role>
 <page>
 <gadget>/desktop/scripts/js/callcontrol.js</gadget>

 <!-- The following gadget is for WXM Customer Experience Journey.
 If WXM is onboarded successfully with all configurations, then replace the url

 with the actual url obtained by exporting the Cisco Finesse gadget from WXM -->

 <!-- <gadget>/3rdpartygadget/files/CXService/CiscoCXJourneyGadget.xml</gadget>
-->
 </page>
 <tabs>
 <tab>
 <id>home</id>
 <icon>home</icon>
 <label>finesse.container.tabs.agent.homeLabel</label>
 <columns>
 <column>
 <gadgets>
 <!-- The following gadget is for recording and displaying Call
Transcripts.
 If Voicea is onboarded successfully and all configuration done
correctly then uncomment this gadget-->
 <!--
-->
<gadget>/3rdpartygadget/files/calltranscript/CallTranscriptGadget.xml</gadget> -->

 <!-- The following gadget is for WXM Customer Experience
Analytics.
 If WXM is onboarded successfully with all configurations, then

```

```

replace the url
 with the actual url obtained by exporting the Cisco Finesse
gadget from WXM -->
 <!--
<gadget>/3rdpartygadget/files/CXService/CiscoCXAnalyticsGadget.xml</gadget> -->

 <gadget>/desktop/scripts/js/queueStatistics.js</gadget>

 <!--
The following Gadgets are for LiveData.
If you wish to show LiveData Reports, then do the following:
1) Uncomment each Gadget you wish to show.
2) Replace all instances of "my-cuic-server.com" with the Fully Qualified
Domain Name of your Intelligence Center Server.
3) [OPTIONAL] Adjust the height of the gadget by changing the
"gadgetHeight" parameter.
IMPORTANT NOTES:
- In order for these Gadgets to work, you must have performed all
documented pre-requisite steps.
- Do *NOT* change the viewId (unless you have built a custom report and
know what you are doing).
- The "teamName" will be automatically replaced with the Team Name of
the User logged into Finesse (for Team-specific layouts).
-->

 <!-- HTTPS Version of LiveData Gadgets -->
 <!-- TEAM STATUS REPORTS: 1. Agent Default view (default), 2.
Agent Skill Group Default view -->
 <!--
<gadget>https://my-cuic-server.com: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> -->
 <!-- QUEUE STATUS REPORTS: 1. Skill Group Default view (default),
2. Skill Group Utilization view, 3. Precision Queue Default view, 4. Precision Queue
Utilization view -->
 <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&

viewId_1=B7371BE210000144000002870A0007C5&filterId_1=skillGroup.id=CL%20teamName&

viewId_2=9E760C8B1000014B0000005A0A0006C4&filterId_2=skillGroup.id=CL%20teamName&

viewId_3=B71A630C10000144000002480A0007C5&filterId_3=precisionQueue.id=CL%20teamName&

viewId_4=286B86F01000014C000005330A0006C4&filterId_4=precisionQueue.id=CL%20teamName</gadget>
-->

 </gadgets>
 </column>
 </columns>
 </tab>
 <tab>
 <id>myStatistics</id>
 <icon>column-chart</icon>
 <label>finesse.container.tabs.agent.myStatisticsLabel</label>
 <columns>
 <column>
 <gadgets>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=150&

```

```

viewId=0B8D11317ED54A80B64F3AE28C5139E5&filterId=agentStats.id=CL%20teamName</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. -->
 <gadgets>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&

viewId=5FA44C6F930C4A64A6775B21A17EED6A&filterId=agentTaskLog.id=CL%20teamName</gadget>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&

viewId=56BC5CCE8C37467EA4D4EFA8371258BC&filterId=agentStateLog.id=CL%20teamName</gadget>

 </gadgets>
 </column>
</columns>
</tab>
<!--
The following Gadgets are for LiveData.
If you wish to show More LiveData Reports, then do the following:
 1) Uncomment each Gadget you wish to show.
 2) Replace all instances of "my-cuic-server.com" with the Fully Qualified Domain Name
of your Intelligence Center Server.
 3) [OPTIONAL] Adjust the height of the gadget by changing the "gadgetHeight" parameter.
IMPORTANT NOTES:
 - In order for these Gadgets to work, you must have performed all documented pre-requisite
steps.
 - Do *NOT* change the viewId (unless you have built a custom report and know what you
are doing).
 - The "teamName" will be automatically replaced with the Team Name of the User logged
into Finesse (for Team-specific layouts).
-->
 <!-- If you are showing the "More Live Data Reports" tab, then also uncomment
this section.
 <tab>
 <id>moreLiveDataReports</id>
 <icon>reports-more</icon>
 <label>finesse.container.tabs.agent.moreLiveDataReportsLabel</label>
 <gadgets>
-->
 <!-- HTTPS Version of LiveData Gadgets -->
 <!-- AGENT REPORTS: 1. Agent Default view (default) -->
 <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&

viewId_1=99E6C8E2100014100000D80A0006C4&filterId_1=agent.id=CL%20teamName</gadget>-->
 <!-- AGENT SKILL GROUP REPORTS: 1. Agent Skill Group Default view (default) -->

```

```

 <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&

viewId_1=9AB7848B10000141000001C50A0006C4&filterId_1=agent.id=CL%20teamName</gadget>-->

 <!-- QUEUE STATUS SKILL GROUP REPORTS: 1. Skill Group Default view (default),
2. Skill Group Utilization view -->
 <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&

viewId_1=B7371BE210000144000002870A0007C5&filterId_1=skillGroup.id=CL%20teamName&

viewId_2=9E760C8B1000014B0000005A0A0006C4&filterId_2=skillGroup.id=CL%20teamName</gadget>-->

 <!-- QUEUE STATUS PRECISION QUEUE REPORTS: 1. Precision Queue Default view
(default), 2. Precision Queue Utilization view -->
 <!--
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&

viewId_1=B71A630C10000144000002480A0007C5&filterId_1=precisionQueue.id=CL%20teamName&

viewId_2=286B86F01000014C000005330A0006C4&filterId_2=precisionQueue.id=CL%20teamName</gadget>-->

 <!-- If you are showing the "more reports" tab, then uncomment this section
too.
 </gadgets>
 </tab>
 -->
 </tabs>
</layout>
<layout>
 <role>Supervisor</role>
 <page>
 <gadget>/desktop/scripts/js/callcontrol.js</gadget>

 <!-- The following gadget is for WXM Customer Experience Journey.
 If WXM is onboarded successfully with all configurations, then replace the url
 with the actual url obtained by exporting the Cisco Finesse gadget from WXM -->

 <!-- <gadget>/3rdpartygadget/files/CXService/CiscoCXJourneyGadget.xml</gadget>
-->
 </page>
 <tabs>
 <tab>
 <id>home</id>
 <icon>home</icon>
 <label>finesse.container.tabs.supervisor.homeLabel</label>
 <columns>
 <column>
 <gadgets>
 <!-- The following gadget is for recording and displaying Call
Transcripts.
 If Voicea is onboarded successfully and all configuration done
correctly then uncomment this gadget-->
 <!--
<gadget>/3rdpartygadget/files/calltranscript/CallTranscriptGadget.xml</gadget> -->

 <!-- The following gadget is for WXM Customer Experience
Analytics.

```



```

 If WXM is onboarded successfully with all configurations, then
replace the url
 with the actual url obtained by exporting the Cisco Finesse
gadget from WXM -->
 <!--
<gadget>/3rdpartygadget/files/CXService/CiscoCXAnalyticsGadget.xml</gadget> -->

 <gadget
id="team-performance">/desktop/scripts/js/teamPerformance.js</gadget>
 <!-- The following gadgets are used for viewing the call history
and state history of an agent selected in the Team Performance Gadget. -->
 <!-- The following gadgets are managed (loaded and displayed)
by the team performance gadget (associated with id "team-performance").
 This association is done using the mapping of managedBy
attribute of the managed gadgets, to the id of managing gadget.
 If the id for team performance gadget is changed, the
values for the associated managedBy attribute
 for the managed gadgets, also need to be updated with the
new id.
 These managed gadgets are not displayed by default, but
would be displayed when the option
 "view history" is selected, for an agent, in the team
performance gadget.
 Note: As managed gadgets are not displayed by default,
placing managed gadgets alone on
 separate columns of their own, would display blank space
in that area.
 For more details on managed gadgets and managedBy attribute,
please refer to Finesse Administration Guide.
-->
 <gadget
managedBy="team-performance">https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=275&
viewId=630CB4C96B0045D9BFF295A49A0BA45E&filterId=agentTaskLog.id=AgentEvent.Id&type=dynamic&maxRows=20</gadget>

 <gadget
managedBy="team-performance">https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=275&
viewId=56BC50CE8C37467EA4D4EFA8371258BC&filterId=agentStateLog.id=AgentEvent.Id&type=dynamic&maxRows=20</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 a logged in supervisor. -->
 <gadgets>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&
viewId=5FA44C6F930C4A64A6775B21A17EED6A&filterId=agentTaskLog.id=CL%20teamName</gadget>

<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=280&

```

```

viewId=56BC5CCE8C37467EA4D4EFA8371258BC&filterId=agentStateLog.id=CL%20teamName</gadget>
 </gadgets>
 </column>
</columns>
</tab>
<tab>
 <id>teamData</id>
 <icon>team-data</icon>
 <label>finesse.container.tabs.supervisor.teamDataLabel</label>
 <columns>
 <column>
 <!-- The following gadget is used by the supervisor to view an
agent's queue interval details. -->
 <gadgets>
<gadget>https://my-cuic-server.com:8444/cuic/gadget/LiveData/LiveDataGadget.jsp?gadgetHeight=310&
viewId=0B8D11317ED54A80B64F3AE28C5139E5&filterId=agentStats.id=CL%20teamName</gadget>
<gadget>https://my-cuic-server.com:8444/cuic/gadget/Historical/HistoricalGadget.jsp?viewId=BD9A8B7DE714E7EB758A9D472F0E7DC&
linkType=htmlType&viewType=Grid&refreshRate=900&@start_date=RELDATE%20THISWEEK&
@end_date=RELDATE%20THISWEEK&@agent_list=CL%20~teams~&gadgetHeight=360</gadget>
 </gadgets>
 </column>
 </columns>
</tab>
<tab>
 <id>queueData</id>
 <icon>storage</icon>
 <label>finesse.container.tabs.supervisor.queueDataLabel</label>
 <columns>
 <column>
 <gadgets>
 <gadget>/desktop/scripts/js/queueStatistics.js</gadget>
 </gadgets>
 </column>
 </columns>
</tab>
</tabs>
</layout>
</finesseLayout>

```

## 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 columns) 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:

**Step 1** Click **Desktop Layout**.

**Step 2** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 3** Enter the product name in the config value tag with title key.

**Step 4** 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 5** 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.

## Customize Desktop Properties

You can customize the Finesse desktop properties.

**Step 1** Click **Desktop Layout**.

**Step 2** Select from the following editors:

- **Text Editor**
- **XML Editor**

**Step 3** Enter the desktop property name in the config key tag.

**Step 4** Enter the possible value of the desktop property in the value tag.

The following are the sample desktop property entries, as displayed in the default **Desktop Layout**. To change these desktop property entries in **Text Editor**, remove the comment (`<!--` and `-->`) and set appropriate values.

```
<!-- <config key="enableDragDropAndResizeGadget" value="false"/> -->
<!-- <config key="wrapUpCountDown" value="true"/> -->
<!-- <config key="desktopChatAttachmentEnabled" value="true"/> -->
<!-- <config key="forceWrapUp" value="true"/> -->
```

The following table lists the supported desktop properties:

Config Key	Value	Default Value
enableDragDropAndResizeGadget	true false	false
enableShortCutKeys	true false	true
forceWrapUp	true false	true
wrapUpCountDown	true false	true
showWrapUpTimer	true false	true
desktopChatAttachmentEnabled	true false	true
desktopChatMaxAttachmentSize	Range: 1—10 (MB)	5
desktopChatUnsupportedFileTypes	Unsupported file formats include comma-separated valid file extensions. For example: .exe, .sh	.exe, .msi, .sh, .bat
showAgentHistoryGadgets	true false	true
showActiveCallDetails (for Supervisor Only)	true false	true
pendingDTMFThresholdCount	Range: 1—20	20
dtmfRequestTimeoutInMs	Range: 1000—200000 (1 to 200 seconds)	5000 (5 seconds)
enableDropParticipantFor	supervisor_only conference_controller_ and_supervisor all	supervisor_only
dropParticipant	agents all	agents

- Note**
- To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES1 COP or higher.
    - pendingDTMFThresholdCount
    - dtmfRequestTimeoutInMs
  - To enable the following Finesse desktop properties in Cisco Finesse, install Cisco Finesse Release 12.5(1) ES4 COP or higher.
    - enableDropParticipantFor
    - dropParticipant

**Step 5** Click **Save**.

The change takes effect when the agent or supervisor refreshes the Finesse desktop or sign out and sign in again.

- Note** If you clear the **Override System Default** check box and click **Save**. The changes are overwritten, and the editing pane reverts to the default desktop layout XML.

---

## 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:

- 
- Step 1** Click **Desktop Layout**.
- Step 2** Select from the following editors:
- **Text Editor**
  - **XML Editor**
- Step 3** Enter name of the gadget or component in the id tag.
- Step 4** Enter the value of the icon in the icon tag.
- Step 5** 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:

```
<tab>
 <id>myHistory</id>
 <icon>/3rdpartygadgets/<some_sample_image>
 <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. -->
 <gadgets>
 <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget
.xml?gadgetHeight=280&viewId=5FA44C6F930C4A64A6775B21A17EED6A&
filterId=agentTaskLog.id=CL%20teamName</gadget>
 <gadget>https://my-cuic-server:8444/cuic/gadget/LiveData/LiveDataGadget
.xml?gadgetHeight=280&viewId=56BC5CCE8C37467EA4D4EFA8371258BC&
filterId=agentStateLog.id=CL%20teamName</gadget>
 </gadgets>
 </column>
 </columns>
</tab>
```

**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
already 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:complexType>
</xs:schema>
```

```

</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" />
 </xs:sequence>
 </xs:complexType>
</xs:element>

```

```

 <!-- 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

---

**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

---

**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

---

- 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

---

- 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

---

- 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

---

- 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 6000 contacts. Import lists that contain more than 6000 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	<b>Note</b> 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.

**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.

- 
- 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, 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




---

**Note** The call variable workflow responds as expected only when you add both the conditions **Is not equal** and **Is not empty**.

---

- 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, its 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.

**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:**

http://www.google.com/search?q=  &  

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.

**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.

**Note** The drop-down list contains variables from all the configured media channels.

**Example:**

The following is the URL example for a Finesse API:

```
/finesse/api/Dialog/ dialogId
```

**Note** When the location is FINESSE, do not specify the protocol, host, and port information. Finesse automatically fetches these details when the REST request is run.

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:

```
<Dialog>
<targetMediaAddress> extension </targetMediaAddress>
<requestedAction>SEND_DTMF</requestedAction>
<actionParams><ActionParam><name>dtmfString</name><value>8</value></ActionParam></actionParam>
</Dialog>
```

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

**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

---

- 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

---

- 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

---

**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

---

**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 260](#).

---

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 176](#).



**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 175](#)

## 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](#).

**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
<b>Type</b>	-	Select a reason type from the drop-down list - <b>Not Ready, Sign Out, Wrap-Up</b> .
<b>Label</b>	Yes	Enter a label for the selected reason type. The field allows maximum of 39 characters. Both alphanumeric and special characters are supported.  <b>Note</b> Enter unique labels for the Wrap-Up reasons.
<b>Code</b>	Yes	Enter a unique code for the selected reason type. The valid range is from 1 to 65535.  <b>Note</b> The <b>Code</b> field is not available for the <b>Wrap-Up</b> reasons.
<b>Description</b>	No	Enter a maximum of 255 characters to describe the reason label.  See <a href="#">Character Sets</a> .

**Step 4** To assign the reason label to one or 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: <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
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

**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
<b>Name</b>	yes	Enter a unique name that will identify the desk settings, using a maximum of 32 alphanumeric characters.
<b>Description</b>	no	Enter a description for the desk settings.
<b>Logout Inactivity Time</b>	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.
<b>Wrapup on Incoming</b>	yes	From the drop-down menu, select <b>Optional</b> (the default), <b>Required</b> , <b>Not Allowed</b> , or <b>Required with wrap-up data</b> to indicate whether the agent is allowed or required to enter wrap-up data after an incoming call. A selection of <b>Optional</b> means the agent can choose to enter wrap-up data or to answer another call.
<b>Wrapup on Outgoing</b>	yes	From the drop-down menu, select <b>Optional</b> (the default), <b>Required</b> , or <b>Not Allowed</b> to indicate whether the agent is allowed or required to enter wrap-up data after an outgoing call. A selection of <b>Optional</b> means the agent can choose to enter wrap-up data or to answer another call.

<b>Wrapup Timer</b>	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.
<b>Supervisor Assist Call Method</b>	no	From the drop-down menu, select either: <ul style="list-style-type: none"> <li>• <b>Consultative Call</b> (default): The caller is aware when the supervisor joins the call. This option is supported in CTI OS and Finesse agent desktops.</li> <li>• <b>Blind Conference</b>: The caller is not aware when the supervisor joins the call. This option is supported only in CTI OS agent desktops.</li> </ul>
<b>Emergency Call Method</b>	no	From the drop-down menu, select either: <ul style="list-style-type: none"> <li>• <b>Consultative Call</b> (default): The caller is aware when the supervisor joins the call. This option is supported in CTI OS and Finesse agent desktops.</li> <li>• <b>Blind Conference</b>: The caller is not aware when the supervisor joins the call. This option is supported only in CTI OS agent desktops.</li> </ul>
<b>Agent State after RONA</b>	no	From the drop-down menu select either: <ul style="list-style-type: none"> <li>• <b>Not Ready</b> (default): The agent is set as not ready after RONA.</li> <li>• <b>Ready</b>: The agent is set as ready after RONA.</li> </ul>
<b>Auto Answer</b>	no	This field represents both Auto Answer and Play Zip tone. Auto Answer will have the following options in the drop-down. From the drop-down menu select either: <ul style="list-style-type: none"> <li>• <b>No Auto Answer</b> In this mode, neither Auto Answer nor Play Zip tone is enabled.</li> <li>• <b>Auto Answer with Zip tone</b>: This mode will allow you to enable both Auto Answer and Play Zip tone.</li> <li>• <b>Auto Answer without Zip tone</b>: This mode will allow you to enable Auto Answer and disable the Play Zip tone.</li> </ul> <p><b>Note</b> This option is not applicable for Mobile agents.</p>

<b>Mobile Agent</b>	no	From the drop-down menu select one of the following: <ul style="list-style-type: none"> <li>• <b>Not Allowed:</b> In this mode, Mobile Agent is not allowed.</li> <li>• <b>Call by Call:</b> 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.</li> <li>• <b>Nailed Up:</b> In this mode, the agent is called at login time and the line stays connected through multiple customer calls.</li> <li>• <b>Agent Chooses:</b> In this mode, an agent can select a call delivery mode at login.</li> </ul>
<b>Enable mobile agent</b>	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.
<b>Require Idle Reason</b>	no	Unchecked by default. When checked, indicates that the agent must enter a reason before entering the Idle state.
<b>Require Logout Reason</b>	no	Unchecked by default. When checked, indicates that the agent must enter a reason before logging out.
<b>ACD shared line usage</b>	no	Unchecked by default. Checked, indicates that the agent will be allowed to log into the devices which have a shared ACD line.  The agent will select the device during the login.

**Note** There is no RONA timer field on the Desk Settings tool. The Query 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

---

- 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

---

- 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](#).

- 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
<b>Type</b>	The read-only type of the Media Routing Domain.
<b>Name</b>	Enter a unique name for the Media Routing Domain.
<b>Description</b>	Enter a description for the Media Routing Domain. See <a href="#">Character Sets</a> .
<b>Service Level Threshold</b>	Enter the maximum time, in seconds, that a customer should wait before being connected with an agent.
<b>Interruptible</b>	Select whether tasks assigned from another MRD can interrupt an agent.  <b>Note</b> 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.
<b>Life</b>	Enter the amount of time, in seconds, that the system waits before ending all tasks if the connection goes down.
<b>Start Timeout</b>	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.
<b>Max Duration</b>	Enter the maximum duration for a task, in seconds.
<b>Max in Queue</b>	Enter the maximum number of tasks allowed to be queued at one time.
<b>Max Time in Queue</b>	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 196

## 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 188](#)).

- 
- 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
<b>Dialed Number String</b>	yes	<p>The value used to route the call or direct the nonvoice task.</p> <p>Enter a string value that is unique for that routing type.</p> <p>Enter a maximum of 24 characters for Post Call Survey (PCS) routing types. For the External Voice routing type, enter a maximum of 24 characters if you're also entering the <b>Ringtone Media File</b> (optional) field. If you're not filling the <b>Ringtone Media File</b> field, enter a maximum of 25 characters. For all other routing types, enter a maximum of 25 characters.</p> <p><b>Note</b> The External Voice and PCS routing types must not have the same dialed number strings.</p>
<b>Description</b>	no	Enter a maximum of 255 characters to describe the dialed number string.
<b>Department</b>	- (yes for departmental administrators)	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<b>Site</b>	-	<p>The <b>Site</b> field displays Main by default for Packaged CCE 2000 Agents deployment.</p> <p>For Packaged CCE 4000 Agents and 12000 Agents deployments, <b>Site</b> is a mandatory field and has no default value.</p> <p>To add a site:</p> <ol style="list-style-type: none"> <li>Click the <b>magnifying glass</b> icon to display the list of sites.</li> <li>Select the required site.</li> </ol>
<b>Peripheral Set</b>	Yes	<p>This field is available only in Packaged CCE 4000 Agents and 12000 Agents deployments. For more information, see <a href="#">Add and Maintain Peripheral Set</a>.</p> <p>To add a peripheral set:</p> <ol style="list-style-type: none"> <li>Click the <b>magnifying glass</b> icon to display the list of peripheral sets configured for the selected <b>Site</b>.</li> <li>Select the required peripheral set.</li> </ol>



Field	Required?	Description
Routing Type	-	

Field	Required?	Description
		<p>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.)</p> <ul style="list-style-type: none"> <li> <p>• <b>External Voice:</b> 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.</p> <p>If you select External Voice, the <b>Ringtone Media File</b> field appears to enter the ringtone filename for the user-defined Dialed Numbers.</p> <p>For remote sites, the <b>External Voice</b> option is available if the site is configured to VRU PG.</p> </li> <li> <p>• <b>Internal Voice:</b> 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.</p> <p>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.</p> <p>Dialed numbers with the routing type Internal Voice appear on the Supervisor Script Dialed Number list when you create or edit a team.</p> <p>For remote sites, the <b>Internal Voice</b> option is available if the site is configured to Agent PG.</p> </li> <li> <p>• <b>Outbound Voice:</b> 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.</p> <p>For remote sites, the <b>Outbound Voice</b> option is available if the site is configured to Multichannel PG.</p> </li> <li> <p>• <b>Post Call Survey:</b> 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 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</p> </li> </ul>

Field	Required?	Description
		<p>Dialed Number and associate the Dialed Number Patterns to the Post Call Survey Dialed Number.</p> <p>For remote sites, the <b>Post Call Survey</b> option is available if the site is configured to VRU PG.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• <b>Customer Collaboration Platform:</b> Select this option for dialed number strings that originate from Customer Collaboration Platform and are routed to an agent who interacts with a customer by Agent Request.</li> <li>• <b>Enterprise Chat and Email:</b> 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.</li> <li>• <b>3rd Party Multichannel:</b> 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.</li> <li>• <b>Digital Routing:</b> Select this option for dialed number strings that originate from Webex Connect application and are routed to the agent who interacts with the customer through digital channels.</li> </ul> <p>See the <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html">https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html</a> for information about configuring the peripherals using Peripheral Gateway Setup.</p>
<b>Media Routing Domain</b>	no	<p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• If the Routing Type is Multichannel, click the <b>magnifying glass</b> icon to display the <b>Select Media Routing Domain</b> popup window.</li> </ul>

Field	Required?	Description
<b>Call Type</b>	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 <b>Overview &gt; Call Settings &gt; Miscellaneous</b> .  To select a different call type: <ul style="list-style-type: none"> <li>• Click the <b>magnifying glass</b> icon to display the <b>Select Call Type</b> popup window.</li> <li>• Click a row to make a selection and close the list.</li> </ul>
<b>PCS Enabled Dialed Number Patterns</b>	no	<b>Note</b> The <b>PCS Enabled Dialed Number Patterns</b> field appears if the <b>Routing Type</b> is <b>Post Call Survey</b> .  Enter one or more dialed number patterns of type External Voice to transfer calls to the Post Call Survey dialed number entered in the <b>Dialed Number String</b> 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.
<b>Ringtone Media File</b>	no	<b>Note</b> The <b>Ringtone Media File</b> field appears if the <b>Routing Type</b> is <b>External Voice</b> .  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.

**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](#).

**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
<b>Routing Pattern</b>	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 (*).
<b>Description</b>	no	Enter a description for the routing pattern. See <a href="#">Character Sets</a> .
<b>Site</b>	-	Displays <b>Main</b> by default. Search and select the routing pattern site.
<b>Pattern Type</b>	yes	Select the type of pattern from the drop-down list.

Field	Required?	Description
Destination	yes	To select the SIP Server Group or FQDN: <b>a.</b> Click the field to open the <b>Add SIP Server Group</b> popup window. Based on the selected <b>Site</b> and <b>Pattern Type</b> , the popup window lists the SIP Server Groups. The SIP Server Groups are configured in <b>Call Settings &gt; Route Settings &gt; SIP Server Group</b> . <b>b.</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. <b>Note</b> Send to originator is not applicable when you select the <b>VRU</b> 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

**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
<b>Location Name</b>	Yes	Enter a name for the location.
<b>Description</b>	No	Enter a description of the location. See <a href="#">Character Sets</a> .
<b>Location Routing Code</b>	Yes	A unique location code that is appended to the ICM label for routing the calls to the destination devices. See <a href="#">Location Properties, on page 192</a> .
<b>Sites</b>	No Required if you add Gateways to the location.	Site of the location. The configured sites with VRU PG are listed in the <b>Sites</b> field. To add sites, select the applicable check boxes in the <b>Sites</b> field.
<b>Gateways</b>	No Required if you select Site(s) for the location.	Gateways that are associated with the location. To associate a gateway to the location: <ol style="list-style-type: none"> <li>Click the + icon. The <b>Add Gateways</b> popup window opens with a list of gateways.</li> <li>Select a gateway from the list. Use the <a href="#">Search a List</a> feature to navigate the list.</li> </ol> <p><b>Note</b> You can view up to 18 servers for a site. Additional server entries will not be displayed and cannot be retrieved via the search feature.</p>

**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.

- 
- 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.

- 
- 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 193

[Add and Maintain SIP Server Group](#), on page 193

[SIP Server Group Properties](#), on page 195

### 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](#).

**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 [ . ].

Field	Required?	Description
Description	no	Enter a maximum of 255 characters to describe the SIP Server Group. See <a href="#">Character Sets</a> .
Site	-	To select the site of the group. Displays <b>Main</b> by default. To select a remote site: <ol style="list-style-type: none"> <li>a. Click the magnifying glass icon to display the list of configured sites.</li> <li>b. Select the required site.</li> </ol>
Type	yes	To select the type of group. From the drop-down list, choose one of the following options: <ul style="list-style-type: none"> <li>• VRU - For Cisco Virtualized Voice Browser (VVB), Cisco Unified SIP Proxy (CUSP), and VXML Gateway devices.</li> <li>• Agent - For Cisco Unified Communications Manager (CUCM) and CUSP devices.</li> <li>• External - For Ingress Gateway and CUSP devices.</li> </ul>

**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.

**Note** You can view up to 25 servers for a site. Additional server entries will not be displayed and cannot be retrieved via the search feature.

- 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

**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
<b>Use Heartbeats to Endpoints</b>	Check the check box to enable the heartbeat mechanism. Heartbeat properties are editable only when this option is enabled. <b>Note</b> Endpoints that are not in a Server Group can not use the heartbeat mechanism.	Enabled (Checked)
<b>Number of Failed Heartbeats for Unreachable Status</b>	The number of failed heartbeats before marking the destination as unreachable.	3
<b>Heartbeat Timeout</b>	The amount of time, in milliseconds, before timing out the heartbeat.	800 milliseconds
<b>Up Endpoint Heartbeat Interval</b>	The ping interval for heart beating an endpoint (status) that is up.	5000 milliseconds

Fields	Description	Default
<b>Down Endpoint Heartbeat Interval</b>	The ping interval for heart beating an endpoint (status) that is down.	5000 milliseconds
<b>Heartbeat Local Listen Port</b>	The heartbeat local socket listen port. Responses to heartbeats are sent to this port on CVP by endpoints.	5067
<b>Heartbeat SIP Method</b>	The heartbeat SIP method.  <b>Note</b> PING is an alternate method; however, some SIP endpoints do not recognize PING and will not respond at all.	OPTIONS
<b>Heartbeat Transport Type</b>	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.  <b>Note</b> TLS transport is not supported.	UDP
<b>Overloaded Response Codes</b>	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
<b>Options Override Host</b>	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 197

[Dialed Number](#), on page 182

## 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](#).

**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 in the **General** tab:

Field	Required?	Description
<b>Name</b>	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.
<b>Description</b>	no	Enter a maximum of 255 characters to describe the call type. See <a href="#">Character Sets</a> .
<b>Service Level Threshold</b>	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 <b>Call Settings &gt; Miscellaneous &gt; Global</b> (see <a href="#">Global</a> , on page 215).  To select a different service level threshold, enter a value in seconds, from 0 to 2,147,483,647.

Field	Required?	Description
<b>Service Level Type</b>	no	<p>Indicates how the system software calculates the service level. The field defaults to the System Default set in <b>Call Settings &gt; Miscellaneous &gt; Global</b> (see <a href="#">Global, on page 215</a>). To override the system default for this call type, select one of these other options from the drop-down menu:</p> <ul style="list-style-type: none"> <li>• <b>Ignore Abandoned Calls:</b> Select this option to excludes abandoned calls from the service level calculation.</li> <li>• <b>Abandoned Calls have Negative Impact:</b> 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.</li> <li>• <b>Abandoned Calls have Positive Impact:</b> 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.</li> </ul>
<b>Bucket Interval</b>	-	<p>Bucket intervals appear in call type reports and display the number of calls answered and abandoned for different time intervals.</p> <p>Configure the bucket interval associated with this call type.</p> <p>The field defaults to the System Default set in <b>Call Settings &gt; Miscellaneous &gt; Global</b> (see <a href="#">Global, on page 215</a>).</p> <p>To select a different bucket interval:</p> <ul style="list-style-type: none"> <li>• Click the <b>magnifying glass</b> icon to display Select Bucket Interval.</li> <li>• Click the row to select a bucket interval and close the List.</li> </ul>
<b>ID</b>	-	<p>This is the system-generated <b>Call Type Id</b>.</p> <p>You cannot edit the Call type Id.</p>

Field	Required?	Description
<b>Enable Experience Management</b>	no	<p>This option will be available only if you have added <b>Cloud Connect</b> in the Inventory page, and configured <b>Webex Experience Management</b>.</p> <p>In case you want to populate the Webex Experience Management survey, you can select the <b>Enable Experience Management</b> check box.</p> <p>The <b>Experience Management</b> tab will be enabled with the following options:-</p> <ul style="list-style-type: none"> <li>• Inline Survey: (post-call voice survey).</li> <li>• Deferred Survey: (post-call Email and SMS survey).</li> </ul> <p><b>Note</b> You can associate only one Survey to a Call Type.</p> <p>Click on the <b>magnifying glass</b> icon, and the configured survey will be populated in the pop-up window.</p>

**Step 5** Click the **Contact Center AI** tab if Cloud Connect is added and registered.

**Step 6** In the **Contact Center AI Configuration** search box, click the search icon. A pop-up window displays a list of available CCAI configurations. Select the required configuration.

**Note** Upon associating the CCAI configuration with the call type, the global configuration (if any) gets overridden for the specific call type.

**Step 7** Click **Save**.

## 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 201

[Sizing Expanded Call Variables](#), on page 204

## 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.

For VRU and media routing leg of the call, the TCD contains the VRU PayloadID setting associated with the peripheral. If not, TCD contains the default payload ID. The Termination Call Variables are persisted only based on this payload setting.

In solutions that only use the default ECC payload, the system doesn't 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 4: 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

**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
<b>Name</b>	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.)
<b>Description</b>	no	Enter up to 255 characters to describe the expanded call variable. There is no restriction of characters.  See <a href="#">Character Sets</a> .
<b>Max Length</b>	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.
<b>Array</b>	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.
<b>Maximum Array Size</b>	no	This field appears when Array is checked. Use it to indicate the maximum number of elements (1-255) in the array.
<b>Enabled</b>	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.
<b>Persistent</b>	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.
<b>Cisco Provided</b>	—	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.
<b>Bytes Required</b> (if enabled)	—	This display-only field indicates the number of bytes required to store the expanded call variable in the system.

Field	Required?	Description
<b>Bytes Required in CTI Server</b> (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.
<b>Total Bytes Required for Enabled Variables: # of maximum 2000 bytes (# bytes remaining)</b>	—	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.
<b>Total Bytes Required for Enabled Variables in CTI Server: # of maximum 2500 bytes (# bytes remaining)</b>	—	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.

**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:  $5 + \text{Maximum\_Length}$
- For array:  $5 + (1 + \text{Maximum\_Length}) * (\text{Maximum\_Array\_Size})$

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  $\text{length of Name} + \text{Maximum Length} + 4$ .
- For an array variable, the size is  $(\text{length of Name} + \text{Maximum Length} + 5) * \text{Maximum Array Size}$ .

## 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

**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
<b>Name</b>	yes	Enter a unique name to identify the script, using a maximum of 32 alphanumeric characters.
<b>Description</b>	no	Enter additional information about the script. See <a href="#">Character Sets</a> .
<b>Routing Type</b>	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).
<b>VRU Script Name</b>	yes	Enter the name of the script as it is known on the Unified CVP. See <a href="#">VRU Script Name Parameters</a> , on page 206.
<b>Configuration Param</b>	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.
<b>RNA Timeout</b>	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.

Field	Required?	Description
<b>Interruptible</b>	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 206
- [Sample VRU Script Names](#), on page 208
- [Configuration Parameters](#), on page 208
- [Sample Configuration Values](#), on page 212

### 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
<p><b>Media File Name</b> options are as follows:</p> <ul style="list-style-type: none"> <li>• A filename--(for instance, a .wav file)</li> <li>• (number 1-10)--Unified CVP plays the file in the corresponding Call.PeripheralVariable file.</li> </ul> <p>For example, a value of 2 instructs Unified CVP to look at Call.PeripheralVariable2.</p> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>	Play Media Get Digits Menu	a is used for PlayMedia only
<p><b>Data Playback Type</b> options are as follows:</p> <ul style="list-style-type: none"> <li>• Number</li> <li>• Char (Character)</li> <li>• Date</li> <li>• Etime (Elapsed time)</li> <li>• TOD (Time of Day)</li> <li>• 24TOD (24-hour Time of Day)</li> <li>• DOW (Day of Week)</li> <li>• Currency (USD only)</li> </ul>	Play Data	
<p><b>Media Library Type Flag</b> indicates the location of the media files to be played. Options are as follows:</p> <ul style="list-style-type: none"> <li>• A--(Default) Application</li> <li>• S--System</li> <li>• V--External VoiceXML</li> </ul>	Play Media Get Digits Menu	V is an option for PlayMedia only.

Parameter Name	Used For	Notes
<b>Uniqueness value</b> (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,0	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
<p><b>Barge-in Allowed</b> Valid options are as follows:</p> <ul style="list-style-type: none"> <li>• Y--Barge-in is allowed.</li> </ul> <p>Note that DTMF barge-in is supported. Voice barge-in is not.</p> <ul style="list-style-type: none"> <li>• N --(Default) Barge-in is not allowed</li> </ul>	Play Media Play Data Get Digits Menu	Unified CVP handles barge-in as follows: <ul style="list-style-type: none"> <li>• 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.</li> <li>• If barge-in is allowed, the H.323Service/Gateway discontinues prompt play when the caller starts entering digits.</li> </ul>
<p><b>DTMF Termination Key</b> A single character that, when entered by the caller, indicates digit entry is complete. Valid options are as follows:</p> <ul style="list-style-type: none"> <li>• 0 to 9</li> <li>• * (asterisk)</li> <li>• # (pound sign, the default)</li> <li>• N (no termination key)</li> </ul>	Get Digits	
<p><b>Incomplete Timeout</b> 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.</p>	Get Digits	V is an option for Play Media only.
<p><b>Inter-digit Timeout</b> The number of seconds the caller is allowed between entering digits. If exceeded, the system times out.</p> <p>The valid options are 1 to 99. The default is 3.</p>	Get Digits	
<p><b>Invalid Entry Message Override</b> The valid options are:</p> <ul style="list-style-type: none"> <li>• Y--Override the system default with a pre-recorded Application Media Library file</li> <li>• N-- (Default) Do not override the system default</li> </ul>	Get Digits Menu	

Parameter Name	Used For	Notes
<p><b>List of Menu Choices</b> Valid options are as follows:</p> <ul style="list-style-type: none"> <li>• 0 to 9</li> <li>• * (asterisk)</li> <li>• # (pound sign)</li> </ul>	Menu	<p>Formats allowed are:</p> <ul style="list-style-type: none"> <li>• Individual options delimited by a / (forward slash)</li> <li>• Ranges delimited by a - (hyphen) with no space</li> </ul>
<p><b>Location of the data to be played</b> Valid options are as follows:</p> <ul style="list-style-type: none"> <li>• Null--(Default) If you leave this option empty, the system uses the expanded call variable named user.microapp.play_data.</li> <li>• A number representing a Call Peripheral Variable number (for example, a 1 to represent Call.PeripheralVariable1).</li> </ul>	Play Data	
<p><b>Maximum Field Length</b> Maximum number of digits entered by the caller. The valid options are 1 to 32. The default is 1.</p>	Get Digits	
<p><b>Minimum Field Length</b> Minimum number of digits entered by the caller. The valid options are 1 to 32. The default is 1.</p>	Get Digits	
<p><b>No Entry Timeout</b> 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.</p>	Get Digits Menu	
<p><b>Number of Invalid Tries</b> 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.</p>	Get Digits Menu	
<p><b>Number of No Entry Tries</b> 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.)</p>	Get Digits Menu	
<p><b>RTSP Timeout</b> 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.</p>	Play Media	

Parameter Name	Used For	Notes
<p><b>Time format</b> Valid only for the time Data Playback types Etime, TOD, and 24TOD.</p> <p>The available formats are as follows:</p> <ul style="list-style-type: none"> <li>• Null--Leave this option empty for non-time formats</li> <li>• HHMM--Default for time formats</li> <li>• HHMMSS</li> <li>• HHMMAP--Includes a.m. or p.m.; valid only for TOD</li> </ul>	Play Data	
<p><b>Timeout Message Override.</b> The valid options are as follows:</p> <ul style="list-style-type: none"> <li>• Y--Override the system default with a pre-recorded Application Media Library file</li> <li>• N--(Default) Do not override the system default</li> </ul>	Get Digits Menu	
<p><b>Type-ahead buffer flush</b> 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:</p> <ul style="list-style-type: none"> <li>• Y—Flush the type-ahead buffer</li> <li>• N—(Default) Do not flush the type-ahead buffer</li> </ul>	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.

**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](#).

- 
- 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: <ul style="list-style-type: none"> <li>• <b>Queued:</b> 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.</li> <li>• <b>Processing:</b> Indicates that the file transfer is being processed.</li> <li>• <b>Succeeded:</b> Indicates that all operations in the file transfer were successful.</li> <li>• <b>Partially Succeeded:</b> Indicates that some operations were successful, and some were unsuccessful.</li> <li>• <b>Failed:</b> Indicates that all operations were unsuccessful.</li> <li>• <b>Cancelled:</b> 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.</li> </ul>
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.

Field	Description
Log File	<p>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.</p> <p>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.</p>

## 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

**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.

Field	Required?	Description
Upper Bound 2 - 9	no	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• All other Upper Bound fields blank. Reports will show the total number of calls answered and calls abandoned after 30 seconds.</li> </ul>

**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

- Login Session

### Congestion Control

You can review congestion control fields in this section. This section contains the following fields:

Field	Description
<b>Congestion Control fields</b>	<ul style="list-style-type: none"> <li>• <b>Treatment Mode</b> This display-only field shows Treat call with DN default label.</li> <li>• <b>System Default Label</b> 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.</li> <li>• <b>Maximum Calls Per Second</b> This display-only field displays the current value for maximum calls per second for the deployment.</li> </ul>

### Agent

Enter values in this section to define system-level values for agents. This section contains the following fields:

Field	Required?	Description
<b>Minimum Password Length</b>	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.
<b>Username Case Sensitivity</b>	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
<b>Bucket Interval</b>	yes	Click the <b>magnifying glass</b> 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 <a href="#">Call Type</a> , on page 196, <a href="#">Skill Groups</a> , on page 105, and <a href="#">Precision Queues</a> , on page 109.)
<b>Call Type</b>	yes	Click the <b>magnifying glass</b> 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 <a href="#">Dialed Number</a> , on page 182.



Field	Required?	Description
<b>Service Level Type</b>	yes	<p>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:</p> <ul style="list-style-type: none"> <li>• <b>Ignore Abandoned Calls:</b> This selection excludes abandoned calls from the service level calculation.</li> <li>• <b>Abandoned Calls have Negative Impact:</b> 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.</li> <li>• <b>Abandoned Calls have Positive Impact:</b> 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.</li> </ul>
<b>Service Level Threshold</b>	yes	<p>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 <a href="#">Call Type</a>, on page 196 and <a href="#">Precision Queues</a>, on page 109.)</p>
<b>Abandon Call Wait Time</b>	yes	<p>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.</p>
<b>Answered Short Call Threshold</b>	no	<p>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.</p>
<b>Reporting Interval</b>	yes	<p>From the drop-down menu, select <b>15 Minutes</b> or <b>30 Minutes</b> 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.</p>

### Script

Use this section to set the number of retained script versions.

Field	Description
<b>Script Versions to Retain</b>	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

Field	Description
<b>Session Inactivity Timer</b>	To set the inactivity timer for the active session, enter the value in minutes. The minimum is 15 minutes and the maximum is 1440 minutes. The default is 30 minutes. When you relogin, the system automatically deletes the inactivity timer value that you had set for the previous 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
<b>Desk Settings</b>	yes	Click the <b>magnifying glass</b> 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 <a href="#">Add and Maintain Agents, on page 77.</a> )
<b>Agent Phone Line Control</b>	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.  <b>Important</b> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>

## Labels

Use this section to view and edit labels for Unified CM, Outbound, and Unified CVP. This section contains the following fields:

Field	Description
<b>Unified CM Label</b>	This field contains a 10 digit string that matches the Unified CM route pattern.
<b>Outbound Label</b>	This field contains a 10 digit string that matches the IOS Voice Gateway dial-peer.
<b>Unified CVP Label</b>	<p>This field contains a 10 digit string that matches the CVP dialed number pattern.</p> <p>When this label is used for all Unified CVP routing clients, the <b>Same Label for All Unified CVPs</b> check box is checked.</p> <p>To use a different label for each Unified CVP routing client, uncheck the <b>Same Label for All Unified CVPs</b> check box, and enter a 10 digit string in each routing client field.</p>

## 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:

### Contact Center AI Configuration

In the Unified CCE Administration console, the Contact Center AI (CCAI) feature tab allows administrators to associate the CCAI configuration (created in the Control Hub at <https://admin.webex.com/>) with all the

call types (global configuration) or with a specific call type. Upon associating a CCAI configuration with the call type, the global configuration (if any) gets overridden for the specific call type.



**Note** To access this feature, add Cloud Connect to the inventory and register it in the Unified CCE Administration console.

## Associate Contact Center AI Configuration with All Call Types

You can view, update, or reset the Contact Center AI configuration, which is associated with all call types.

### *View Contact Center AI Configuration*

In the **Unified CCE Administration**, navigate to **Overview > Features > Contact Center AI**. The **Contact Center AI Configuration** search box displays the name of the CCAI configuration that was previously associated with all call types.

### *Reset Contact Center AI Global Configuration*

This procedure explains how to reset the Contact Center AI configuration. Upon reset, the previously associated configuration is cleared from the search box.

- 
- Step 1** In the **Unified CCE Administration**, navigate to **Overview > Features > Contact Center AI**.
- Step 2** In the **Contact Center AI Configuration** search box, next to the configuration name, click the **x** icon.
- Step 3** Click **Save**.
- 

## Manage digital channels



**Note** To access this feature, ensure that you add Cloud Connect to the inventory in the Unified CCE Administration portal and register it.

As an administrator, perform the following configurations in the Unified CCE Administration portal to manage digital channel capabilities for your customers to reach business:

- Set up media channels such as chat, email, social, voice callback, . See [Set up media channels, on page 221](#).
- Synchronize agents in AW database to Webex Engage database. See [Configure User Sync, on page 223](#).
- Define Expanded Call Context (ECC) variables to assist agents with relevant information. See [Define ECC variables](#).
- Integrate Cloud Connect with Webex Connect using the Open Authorization v2.0 (OAuth v2.0) standard. See [Integrate Cloud Connect with Webex Connect](#).
- Customize the connection parameters between Cloud Connect and MR PG. See [Manage connection between Cloud Connect and MR PG, on page 225](#).

## Set up media channels

Contact Center Enterprise (CCE) supports media channels, such as Live Chat, Email, and SMS, with enhanced capabilities. These media channels are mapped to media type and Media Routing Domains (MRDs) for providing granular channel-specific reporting and agent state control. Based on this configuration, Cloud Connect associates the received task request to the appropriate MRD.

MRDs are used to map agents' skill group with the media channels, based on which the agents are assigned a task. You can map multiple media channels to the same MRD. For example, you can map SMS and Chat channels to the same MRD. For more information on MRDs, see the *Media Routing Domains* section in the [Configuration Guide for Cisco Unified ICM Enterprise](#).

Media type is a broad category of media channels and it is different from the media class or MRD in CCE. The Digital Routing service has internal sub-limits and different maximum queue time parameters that it applies for tasks of a certain Media Type as defined by the Queue Settings. The media types are **Chat**, **Email**, **Telephony** (Voice Callback), **Social**, , and .

Webex Connect offers support for the pre-provisioned system defined media channels. You can add a custom media channel if one of the many media channels that Webex Connect supports in the future has to be allowed in the CCE system. If not, you can skip adding a Media Channel.



**Note** System-defined media channels cannot be deleted.

**Queue Settings** for media channels is used to configure the maximum queue limit and maximum queue time for each media type, individually. For more information on configuring queue settings for media channels, see [Configure queue settings](#).

To set up media channels:

**Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Media Channel**. The list of existing media channels is displayed in a grid. This is the default page.

**Step 2** Click **New**. On the **New Media Channel** page, do the following:

- a) In the **Name** field, type the name of the media channel.
- b) From the **Media Type** drop-down list, select the required media type.
- c) In the **Media Routing Domain** field, search and select the MRD that you want to map to the media channel.

**Step 3** Click **Save**. The channel is added to the list on the **Digital Channel Settings** page.

When you have created a media channel, you can modify only the **Media Routing Domain** field. If you want to modify any other fields, you must delete the media channel and create afresh. To delete a media channel, hover over the media channel and click the **X** icon.

### Configure queue settings

The Digital Routing service maintains a queue for all the incoming tasks. The service accommodates up to a maximum of 100,000 tasks in the queue at any given point in time. Out of these 100,000 tasks, you can configure the maximum number of tasks that can be queued for each media type in the Digital Routing service. The following are the default values in percentage for each media channel:

Media type	Queue setting in %	Description
Email	50%	50,000 tasks can be queued for Email.
Social	40%	40,000 tasks can be queued for SMS.
Voice callback	5%	5,000 tasks can be queued for Voice callbacks.
Chat	5%	5,000 tasks can be queued for live chat.

You can also define the maximum duration for which a task remains in the queue for each media type.

The following are the scenarios in which the Digital Routing service rejects the tasks and sends them back to Webex Connect:

- The number of tasks exceeds the maximum value that is configured for the media channel. For example, consider that the Digital Routing service queue has 50,000 email tasks, which is the maximum queue setting defined for the Email media channel. If Webex Connect further injects email tasks, the Digital Routing service rejects the incoming tasks and sends them back to Webex Connect with an error code of 20286 (MEDIA\_TYPE\_QUEUE\_LIMIT\_EXCEEDED). For example, a flow developer can decide to provide appropriate messaging to the end customer and invoke other backend systems to denote queue capacity issues.
- A task exceeds the maximum duration that is defined for the media channel. The Create Task node is successful. There is a Closed webhook event triggered when the task gets auto-closed after exceeding the maximum time in queue, with a specific disposition code set to CD\_MAX\_DIALOG\_LIFETIME\_EXCEEDED.

The flow debug logs show the error code returned by the Create Task node API call. For more information about the Create Task node, see [Create Task](#).

To configure the queue settings for the media channels:

- 
- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Media Channel**.
- Step 2** Click **Queue Settings**.
- Step 3** Enter the required values in percentage for each media channel.
- Note** Make sure that the sum of the percentage values configured for all the media channels is 100.
- Step 4** Define the duration in days, hours, and minutes for each media channel. This is the maximum duration for which a task that belongs to the specific media channel remains in the queue after which it gets timed out. The default durations are 3 days for Email and Social media channels, and 2 hours for Voice callbacks and Chat media channels.
- Step 5** Click **Save**.
-

## Configure User Sync

To synchronize the CCE agents who are configured for digital channel interactions with Webex Connect:

- 
- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > User Sync**.
- Note** The DataConn service is active only on the publisher node of Cloud Connect. Ensure that the publisher node is accessible for you to view the **User Sync** page.
- Step 2** In the **Network Entry Point** field, enter the hostname or FQDN of the load balancer or the reverse proxy server based on your deployment. It is through this network entry point that the Webex Engage sends the response request to the DataConn service for agent synchronization.
- For more information about network entry point, see the *Synchronize CCE agents to Webex Engage* section in the [Solution Design Guide for Cisco Unified Contact Center Enterprise Solution Design Guide for Cisco Packaged Contact Center Enterprise](#).
- Step 3** In the **AW Database Details** area, complete the following fields to configure the DataConn service for the Primary and the Secondary Server:
- In the **AW Datasource Host** field, enter the IP address or the host name of the AW server that has the agent configurations.
  - In the **Port** field, enter the SQL port number of the AW database server.
  - In the **Database Name field**, enter the name of the AW database server.
  - In the **Database User ID** and **Password** fields, enter the user ID and password of the SQL user account that you created for digital channels. For more information see the *Configure SQL user account for digital channels* section in the [Cisco Unified Contact Center Enterprise Features GuideCisco Packaged Contact Center Enterprise Features Guide](#).
- Step 4** Click **Test Connection** to make sure that the DataConn service can read the data from the AW Primary server.
- Step 5** Switch on the **Enable Failover** toggle button to enable the failover to the Secondary AW server.
- Step 6** To synchronize agents, choose one of the following options:
- Enable the **Enable Sync** toggle button to automatically synchronize agents in an interval of 30 minutes.
  - Click **Sync Now** to manually synchronize the agents. This option is available only when the **Current Sync Status** field appears as **Scheduled**.
- Note** If you recreate your AW Database to fix any errors, ensure that you disable User Sync before starting with the recreation process. Enable the User Sync only after the AW Database is created and synchronized with the central controller database.
- Step 7** In the **Last sync** field, view the date, time and status of the previous synchronization.
- Step 8** In the **Agents Sync Details** field, view the number of agents that are synchronized successfully. The number of agents appears as a clickable link. Click the link to view the list of agent records that have failed to synchronize and the list of agent records that are pending for synchronization. You can choose to refresh the agent records at any given point in time.
- Step 9** In the **Current Sync Status** field, you can view one of the following statuses:
- No sync is in progress or scheduled**—This status appears when the **Enable Sync** toggle button is off.
  - Scheduled**—This status appears when the **Enable Sync** toggle button is on.

- c. **In Progress**—This status appears when the scheduled sync or manual sync is in progress.
- d. **Manual Sync Failed** —This status appears when the manual sync has failed.
- e. **Unknown**—When sync status is not available.

**Step 10** Click **Save**.

---

## Define ECC variables

The Expanded Call Context (ECC) variables are data that are embedded within the call and are visible to the agent on the Agent Desktop. ECC variables are passed back and forth in ECC payloads. ECC variables assist the agent with relevant information without the customer having to repeat the same information.

To define the ECC variables:

---

- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > ECC Variable**.
  - Step 2** On the **ECC Variable** page, click the plus icon (+). The **Add ECC Variable** page appears with existing variables **Name** and **Enabled** details. It excludes the built-in variables.
  - Step 3** Select the required variable. The **ECC Variable** page displays the newly added ECC variable.
  - Step 4** Click **Save**.
- 

## Integrate Cloud Connect with Webex Connect

You can integrate Cloud Connect with Webex Connect using the Open Authorization v2.0 (OAuth v2.0) standard. You must configure Webex Connect client ID and client secret in the Digital Routing service for the service to gain access to Webex Connect using the access token. This set of client credentials uniquely identifies the Cloud Connect and its permissions to access Webex Connect.



**Note** The Cloud Connect Management service is active only on the publisher node of Cloud Connect.

---

To configure client credentials for OAuth v2.0 access token:

---

- Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Integration**.
- Step 2** On the **OAuth2 Authentication Details** page, perform the following steps.
  - a) In the **Name** field, enter a name for the Cloud Connect integration. This field is editable.
  - b) In the **Description** field, enter a description of what the client application does.
  - c) In the **Client Id** and **Client Secret** fields, enter the client id and secret key that you can retrieve from the Webex Connect portal (navigate to **Assets > Integrations > CCE pre-built integrations > Actions > Manage**).
  - d) In the field, enter the password that is provided to you at the time of registration. This is the secret key that was used for generating the token.
  - e) In the **Token Request URL** field, provide one of the following URLs based on the location of Webex Connect datacenter:



- Ireland—[https://keycloak-authservice.imiconnect.io/auth/realms/imiconnect\\_uk\\_prod/token](https://keycloak-authservice.imiconnect.io/auth/realms/imiconnect_uk_prod/token)
- London—[https://keycloak-authservice.imiconnect.eu/auth/realms/imiconnect\\_in\\_prod/token](https://keycloak-authservice.imiconnect.eu/auth/realms/imiconnect_in_prod/token)
- Sydney—[https://keycloak-authservice.imiconnect.com.au/auth/realms/imiconnect\\_syd\\_prod/token](https://keycloak-authservice.imiconnect.com.au/auth/realms/imiconnect_syd_prod/token)
- The United States of America—[https://keycloak-authservice-us.imiconnect.io/auth/realms/imiconnect\\_us\\_prod/token](https://keycloak-authservice-us.imiconnect.io/auth/realms/imiconnect_us_prod/token)
- Canada—[https://keycloak-authservice.imiconnect.ca/auth/realms/imiconnect\\_cn\\_prod/token](https://keycloak-authservice.imiconnect.ca/auth/realms/imiconnect_cn_prod/token)

- f) From the **Method** drop-down list, select the **POST** method for Webex Connect integration.
- g) From the **Content Type** drop-down list, select a media content type. This determines the response format. The available options are **application/json**, **application/xml**, and **application/x-www-form-urlencoded**. For Webex Connect integration, select **application/x-www-form-urlencoded**.
- h) In the **Access Token JSON path**, enter the path in the JSON response to fetch the value of the access token. For the Webex Connect integration, enter *access\_token*.
- i) (Optional) In the **Header List** section, click + icon to add a header name and value and click **Add**. The header name and value are used to pass any additional information that Webex Connect may require for Cloud Connect integration.

**Step 3** Click **Save** to save the OAuth2 authentication details.

**Step 4** Go to the **Webhook** tab to register the Webhook URL in the Digital Routing service. To fetch the Webhook URL:

- a) In the Webex Connect portal, navigate to **Assets > Integrations**.
- b) In the CCE pre-built integrations row, from the **Actions** column, select **Manage**. The **Manage Integration - Prebuilt Integration** page appears.
- c) In the **Inbound Events** section, copy the Webhook URL.

**Step 5** Paste the URL in the **Webhook URL** field in the Unified CCE Administration portal (**Overview > Digital Channels > Digital Channel Settings > Integration > Webhook**).

---

## Manage connection between Cloud Connect and MR PG

To customize the connection parameters between Cloud Connect and Media Routing Peripheral Gateway (MR PG):

**Step 1** In the Unified CCE Administration portal, navigate to **Overview > Digital Channels > Digital Channel Settings > Advanced Settings**.

**Step 2** The **Port** is a display-only field and the default value is **38001**. It is through this port that Cloud Connect and MR PG communicates with each other.

**Step 3** The **Secured** toggle switch is turned on by default. It is to establish a secured connection between Cloud Connect and MR PG. You can turn-off this toggle switch to disable the secure connection.

**Step 4** Click **Save**.

---

## 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>.

- 
- 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
<b>Maximum Callbacks per Dialed Number</b>	Yes	<p>By default, the <b>Unlimited</b> option is selected, which is equivalent to an unlimited number of callbacks offered per calling number. The maximum value is 1000.</p> <p>To limit the number of calls, from the same calling number that are eligible to receive a callback:</p> <ol style="list-style-type: none"> <li>a. Select the <b>Limited</b> option.</li> <li>b. Enter a positive number in the text field to allow Courtesy Callback to validate and allow the specified number of callbacks per calling number.</li> </ol>

Fields	Required?	Description
<b>Allow unmatched Dialed Numbers</b>	No	<p>Check the <b>Allow unmatched Dialed Numbers</b> check box to allow callbacks to the dialed numbers that are not available in the <b>Allowed Dialed Number Patterns</b> list.</p> <p><b>Note</b> If no dialed numbers are present in the <b>Allowed Dialed Number Patterns</b> list, then Courtesy Callback does not allow any callbacks.</p>
<b>Allowed Dialed Number Patterns</b>	No	<p>The list of allowed dialed numbers to which callbacks can be sent. By default, the list includes preconfigured allowed dialed number patterns.</p> <p>To add a dialed number pattern:</p> <ol style="list-style-type: none"> <li>a. Click the '+' icon and enter a dialed number pattern. Valid characters are alphanumeric, period (.), Exclamation (!), asterisk(*), greater than(&gt;), and backslash (\). The field does not allow you to enter any invalid characters.</li> <li>b. Click <b>Add</b>.</li> </ol> <p>To remove a dialed number pattern, click the 'x' icon associated with the number in the list.</p>

Fields	Required?	Description
<b>Denied Dialed Number Patterns</b>	No	<p>The list of denied dialed numbers to which callbacks are never sent.</p> <p>By default, the list includes preconfigured denied dialed number patterns.</p> <p>To add a dialed number pattern:</p> <ol style="list-style-type: none"> <li>a. Click the '+' icon and enter a dialed number pattern. <ul style="list-style-type: none"> <li>Valid characters are alphanumeric, period (.), Exclamation (!), asterisk(*), greater than(&gt;), and backslash (\). The field does not allow you to enter any invalid characters.</li> </ul> </li> <li>b. Click <b>Add</b>.</li> </ol> <p>To remove a dialed number pattern, click the 'x' icon associated with the number in the list.</p> <p>Denied numbers take precedence over allowed numbers.</p> <ul style="list-style-type: none"> <li>• Wildcarded DN patterns can contain "." and "X" in any position to match a single wildcard character.</li> <li>• Any of the wildcard characters in the set "&gt;*" matches multiple characters but can only be used trailing values because they always match all remaining characters in the string.</li> <li>• The highest precedence of pattern matching is an exact match, followed by the most specific wildcard match.</li> <li>• 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.</li> </ul>

**Step 5** 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>

## Third-party Integration



---

**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 233](#).

### 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 231](#)

## 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 interface 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.

**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
<b>General Tab</b>	
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.  <b>Note</b> 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.
System Defined Data	Optional. Define data that the third-party user interface can use while its rendered. Click + and select from the following list. <ul style="list-style-type: none"> <li>• <b>Deployment Type:</b> The current deployment type.</li> <li>• <b>Current User:</b> The credentials of the logged on user.</li> <li>• <b>Current Role:</b> The role of the logged on user.</li> <li>• <b>API-based URL:</b> The base URL on to which the APIs are loaded.</li> <li>• <b>Locale:</b> The current locale setting.</li> </ul>
User Defined Data	Optional. Define custom key-value pairs you need to render the third-party user interface. To add a key-value pair: <ol style="list-style-type: none"> <li>a. Click +.</li> <li>b. Enter the name and value in the respective fields.  <b>Note</b> The <b>Value</b> field is optional. You can only enter up to 1024 characters in the <b>Value</b> field.</li> <li>c. Optional. Hide the value you enter by selecting the <b>Mask</b> check box.</li> <li>d. Click ✓ to add.</li> <li>e. To add another parameter, click + again.</li> </ol>



**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 231](#)

*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.

---

**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.

---

**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
<b>General Tab</b>	
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.
System Defined Data	<p>Optional. Define data that the third-party user interface can use while its rendered. Click + and select from the following list.</p> <ul style="list-style-type: none"> <li>• <b>Deployment Type:</b> The current deployment type.</li> <li>• <b>Current User:</b> The credentials of the logged on user.</li> <li>• <b>Current Role:</b> The role of the logged on user.</li> <li>• <b>API-based URL:</b> The base URL on to which the APIs are loaded.</li> <li>• <b>Locale:</b> The current locale setting.</li> </ul> <p>For more information, see the <i>Cisco Packaged Contact Center Enterprise Developer Reference Guide</i></p>
User Defined Data	<p>Optional. Define custom key-value pairs you need to render the third-party user interface. To add a key-value pair:</p> <ol style="list-style-type: none"> <li>a. Click +.</li> <li>b. Enter the name and value in the respective fields. <ul style="list-style-type: none"> <li><b>Note</b>      The <b>Value</b> field is optional. You can only enter up to 1024 characters in the <b>Value</b> field.</li> </ul> </li> <li>c. Optional. Hide the value you enter by selecting the <b>Mask</b> check box.</li> <li>d. Click ✓ to add.</li> <li>e. To add another parameter, click + again.</li> </ol>

**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.

---

**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.

---

**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 234
- Add, rename, and delete menus in system-defined cards. For details, see [Manage System-Defined Cards](#) , on page 235




---

**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.



---

**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:





- Click the **Add New Card** card.

**Note** The **Add New Card** card is disabled after you have added eight cards.

- Click  to choose a color and icon for the card.
- Click  next to **Add Title** to enter the card title.
- 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.

**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.

---

## Customer Virtual Assistant

Customer Virtual Assistant (CVA) enables the IVR Platform to integrate with cloud-based speech services. CVA provides the following speech services:

- **Text-to-Speech:** Integration with cloud-based TTS services in your application for Speech Synthesis operations. CVA currently supports Google Text-to-Speech service.
- **Speech-to-Text:** Integration with cloud-based ASR services in your application for Speech Recognition operations. CVA currently supports Google Speech-to-Text service.
- **Speech-to-Intent:** CVA provides capability of identifying the intent of customer utterances by processing the text received from Speech-to-Text operations. CVA offers this service by using cloud-based Natural Language Understanding (NLU) services. CVA currently supports Google Dialogflow service.

For more information, see *Customer Virtual Assistant* chapter in *Feature Guide for Cisco Unified Contact Center* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-customer-voice-portal/tsd-products-support-series-home.html>.

You can configure and manage speech services using the **Unified CCE Administration > Overview > Features > Customer Virtual Assistant** page.

This page contains the following tabs to configure speech services:

- **Text to Speech:** Go to this tab to configure TTS service accounts.
- **Automatic Speech Recognition:** Go to this tab to configure ASR service accounts.
- **Natural Language Understanding:** Go to this tab to configure NLU service accounts.

## Text to Speech

Text to Speech (TTS) tab enables you to view, add, edit, or delete TTS service accounts.

### Related Topics

[Customer Virtual Assistant](#)

### *Add and Maintain Text to Speech Account*

This procedure explains how to add a text to speech account. For more information on maintaining service accounts, see [Edit Text to Speech Service Account, on page 236](#) and [Delete Service Account, on page 238](#).

- 
- Step 1** Click the **Text to Speech** tab.
- Step 2** Click **New** to open the **New Text to Speech Account** pop-up.
- Step 3** Complete the fields.  
For more information, see [Field Details for Text to Speech Service Provider, on page 239](#).
- Step 4** Click **Next** to continue.
- Step 5** Complete the fields that are displayed based on the selected service provider.
- Step 6** Click **Save**.
- 

### *Edit Text to Speech Service Account*

This procedure explains how to edit configuration details for a Text to Speech account.




---

**Note** Any change in configuration takes effect after 5 minutes.

---

- 
- Step 1** Click the **Text to Speech** tab.
- Step 2** Click the service account for which you want to edit the configuration.  
The **Edit** section opens for the selected service account.
- Step 3** Edit the required fields.  
For more information, see [Field Details for Text to Speech Service Provider, on page 239](#).

**Step 4** Click **Save**.

---

## Automatic Speech Recognition

Automatic Speech Recognition (ASR) tab enables you to view, add, edit, or delete ASR service accounts.

### Related Topics

[Customer Virtual Assistant](#)

### *Add and Maintain Automatic Speech Recognition Account*

This procedure explains how to add an Automatic Speech Recognition account. For more information on maintaining service accounts, see [Edit Automatic Speech Recognition Service Account, on page 237](#) and [Delete Service Account, on page 238](#).

---

**Step 1** Click the **Automatic Speech Recognition** tab.

**Step 2** Click **New** to open the **New Automatic Speech Recognition** pop-up.

**Step 3** Complete the fields.

For more information, see [Field Details for Automatic Speech Recognition Service Provider, on page 240](#).

**Step 4** Click **Next** to continue.

**Step 5** Complete the fields that are displayed based on the selected service provider.

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

---

### *Edit Automatic Speech Recognition Service Account*

This procedure explains how to edit configuration details for an Automatic Speech Recognition account.



**Note** Any change in configuration takes effect after 5 minutes.

---

**Step 1** Click the **Automatic Speech Recognition** tab.

**Step 2** Click the service account for which you want to edit the configuration.

The **Edit** section opens for the selected service account.

**Step 3** Edit the required fields.

For more information, see [Field Details for Automatic Speech Recognition Service Provider, on page 240](#).

**Step 4** Click **Save**.

---

## Natural Language Understanding

Natural Language Understanding (NLU) tab enables you to view, add, edit, or delete NLU service accounts.

**Related Topics**[Customer Virtual Assistant](#)*Add and Maintain Natural Language Understanding Account*

This procedure explains how to add a Natural Language Understanding (NLU) account. For more information on maintaining service accounts, see [Edit Natural Language Understanding Service Account, on page 238](#) and [Delete Service Account, on page 238](#).

- 
- Step 1** Click the **Natural Language Understanding** tab.
- Step 2** Click **New** to open the **New Natural Language Understanding** pop-up.
- Step 3** Complete the fields.  
For more information, see [Field Details for Natural Language Understanding Service Provider, on page 241](#).
- Step 4** Click **Next** to continue.
- Step 5** Complete the fields that are displayed based on the selected service provider.
- Step 6** Click **Save**.
- 

*Edit Natural Language Understanding Service Account*

This procedure explains how to edit configuration details for a Natural Language Understanding account.




---

**Note** Any change in configuration takes effect after 5 minutes.

---

- 
- Step 1** Click the **Natural Language Understanding** tab.
- Step 2** Click the service account for which you want to edit the configuration.  
The **Edit** section opens for the selected service account.
- Step 3** Edit the required fields.  
For more information, see [Field Details for Natural Language Understanding Service Provider, on page 241](#).
- Step 4** Click **Save**.
- 

**Delete Service Account**

- 
- Step 1** Hover the mouse pointer over the row of the service account to be deleted. Click the **x** icon at the end of the row.
- Step 2** Click **Yes** to confirm.
-

## Supported Fields from Service Provider

### Field Details for Text to Speech Service Provider

Service Provider	Field	Required?	Editable?	Description
Google	<b>Service Account</b>	Yes	Yes (only for adding a service account)	Unique identifier for the service account <sup>1</sup> .  This should match the name of the account created in Google.
	<b>Service Provider</b>	Yes	No	Name of the service provider.
	<b>Description</b>	No	Yes	Short description of the service account.
	<b>Set as Default</b>	No	Yes	Makes the service account default. Toggle to turn on/off the <b>Set as Default</b> . Only one service account can be set as default for a given service.
	<b>Service Account Key</b>	Yes	Yes	Service account key <sup>2</sup> of the service account.

<sup>1</sup> Use the same Service Account name in the Call Studio.

<sup>2</sup> Use the key provided in the .json file. For more information on how to fetch the .json file from the service provider, see <https://cloud.google.com/text-to-speech/docs/quickstart-client-libraries>. CCAI customers must use the key provided during the onboarding process.

## Field Details for Automatic Speech Recognition Service Provider

Service Provider	Field	Required?	Editable?	Description
Google	<b>Service Account</b>	Yes	Yes (only for adding a service account)	Unique identifier for the service account <sup>3</sup> .  This should match the name of the account created in Google.
	<b>Service Provider</b>	Yes	No	Name of the service provider.
	<b>Description</b>	No	Yes	Short description of the service account.
	<b>Set as Default</b>	No	Yes	Makes the service account default. Toggle to turn on/off the <b>Set as Default</b> . Only one service account can be set as default for a given service.
	<b>Service Account Key</b>	Yes	Yes	Service account key <sup>4</sup> of the service account.

<sup>3</sup> Use the same Service Account name in the Call Studio.

<sup>4</sup> Use the key provided in the `.json` file. For more information on how to fetch the `.json` file from the service provider, see <https://cloud.google.com/speech-to-text/docs/quickstart-client-libraries>. CCAI customers must use the key provided during the onboarding process.



*Field Details for Natural Language Understanding Service Provider*

Service Provider	Field	Required?	Editable?	Description
Dialogflow	<b>Service Account</b>	Yes	Yes (only for adding a service account)	Unique identifier for the service account <sup>5</sup> . This should match the name of the account created for Dialogflow.
	<b>Service Provider</b>	Yes	No	Name of the service provider.
	<b>Description</b>	No	Yes	Short description of the service account.
	<b>Service Account Key</b>	Yes	Yes	Service account key <sup>6</sup> of the service account.

<sup>5</sup> Use the same Service Account name in the Call Studio.

<sup>6</sup> Use the key provided in the `.json` file. For more information on how to fetch the `.json` file from the service provider, see <https://dialogflow.com/docs/reference/v2-auth-setup>. CCAI customers must use the key provided during the onboarding process.

## Cloud Connect Administration

Cloud Connect is a component that hosts services that allow customers to use cloud capabilities such as Cisco Webex Experience Management, VAV Transcript, Agent Answers, Call Transcription, Digital Channel, and CCE Orchestration.

### Configure Cloud Connect

Follow this procedure to add Cloud Connect Publisher as an external machine.

#### Before you begin

Import the Cloud Connect certificate to AW. For details on how to do this, see the Import VOS Components Certificate topic.

- 
- Step 1** From Unified CCE Administration, navigate to **Infrastructure Settings > Inventory > External Machines**. The **Add Machine** page appears.
  - Step 2** From the **Type** drop-down list, select **Cloud Connect Publisher**.
  - Step 3** In the **Hostname/IP Address** field, enter the IP address or hostname of the Cloud Connect device.
  - Step 4** In the Cloud Connect Administration tab, enter the user name and password of the Cloud Connect device. The Cloud Connect Publisher is added to the Packaged CCE Inventory.
  - Step 5** The Cloud Connect Subscriber is auto-discovered. Log into **Unified CCE Administration** again if the subscriber is not discovered automatically.

**Step 6** The Cloud Connect details is sent to the CVP and Finesse devices in the inventory.

## Cloud Connect Integration

To navigate to the **Cloud Connect Integration** page follow the steps:

**Step 1** In **Unified CCE Administration**, choose **Overview > Features > Cloud Connect Integration**.

**Step 2** On **Cloud Connect Integration** page, registration information is displayed. To register or deregister click **Cisco Webex**.

Field	Required?	Description
<b>Registration</b>		
Registration	-	Cloud Connect registration status of Control Hub will be displayed.
<b>Cisco Webex</b>		
Cisco Webex	-	On <b>Cloud Connect Integration</b> , if you click the <b>Cisco Webex</b> link, you will be re-directed to Cisco Webex login page.
<b>Cluster Information</b>		
Proxy Details	NO	Enter the proxy details used by the Cloud Connect. For example: abc.cisco.com:8080 <b>Note</b> By default, HTTP uses the <b>port 80</b> , but you can specify a different port number in the proxy.
Deployment ID	-	Read-only field that displays the Deployment ID, an auto-generated identifier of the Unified CCE instance.
Deployment Name	NO	Enter a valid deployment name.

## Configuring Cloud Connect Node

*set cloudconnect cherrypoint config*

**Required Minimum Privilege Level:** Advanced

**Command Default** Run this command to update the Cloud Connect Cherry point connector configuration details.



**Note** When you run this command, you are prompted to enter new configuration details. The current configuration details are displayed within [ ]. You can enter the new configuration details or retain the existing configuration.



**Note** User input for Web URL Prefix must be a valid http or https URL. The default value is https://nps.bz . For users upgrading Cloud Connect, if the Web URL prefix does not have a valid http or https URL prefix, they must reconfigure Cloud Connect Cherry point to provide a valid URL for Web URL prefix.

When reconfiguring the Web URL prefix, ensure all the inputs are re-entered again.



**Note** **Voice PIN Prefix, SIP URI Domain** are no more applicable and the user will not be prompted for the same and will not be shown in the CLI command output.

### Command Syntax

#### set cloudconnect cherrypoint config

When you run this command, the current Cloud Connect Cherry point connector configuration is fetched and is displayed. You are prompted to enter new configuration details. The current configuration details are displayed within `[ ]`. You can enter the new configuration details or retain the existing configuration.

Example:

```
admin:set cloudconnect cherrypoint config
Fetching existing configuration...
Enter the Config details to be saved:
Desktop User (with Read Only Privileges): readonlyusername
Desktop User API Key []: apikey-ABCD1234EFGH5789!dummy
System User (with Read and Write Privileges): reawriteusername
System User API Key []: apikey-JKMLN012345OPQRST6789!dummy
Web URL Prefix: https://nps.bz
Deployment ID: CCE_Deployment_Bangalore_Site
Proxy Enabled(true/false) [false]: true
Proxy Host: proxyhost.domain.com
Proxy Port [0]: 5678
The config details updated successfully.
```

## 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.
- A Contact Center AI job content file contains cells for agentId, userName, and agentServices. Entering content in those cells will enable or disable Contact Center AI services for the agents.




---

**Note** The Contact Center AI job content file is available only when Cloud Connect is added in the inventory.

---




---

**Note** Avoid performing a bulk job transaction during a maintenance window.

---




---

**Note** Limit the bulk job import to 1000 records at any given instance.

---




---

**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.

- 
- 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 Contact Center AI Services Content File

The content file for Contact Center AI bulk job contains the fields given in the following table. Enter the values appropriately in the given fields to enable or disable Contact Center AI Services for the agents.



**Note** Bulk job is available for administrators only when Cloud Connect is added in the inventory and registered on the Control Hub.

Field	Required?	Description
agentId	Agent ID or Username	Existing agentId for which you want to enable or disable the Contact Center AI Services.  You must provide either an agentId or the userName. If both are provided, agentId takes precedence over the userName. If the agentId value is left blank, the userName will reference an existing agent.
userName	Username or Agent ID	Username of the agent for which you want to enable or disable the Contact Center AI Services.  If no agent is found with the given username, the Contact Center AI Services association fails.
agentServices	Yes (to enable Contact Center AI Services)	The type of Contact Center AI Services to be associated with the agent. Supported values are AgentAnswers, VAV Transcript, and Transcript. To associate more than one services, separate the values using semicolon (;).  If the value is updated, any existing enabled service gets overwritten. If the value is left empty, no service gets associated with the agent.

### 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): <ul style="list-style-type: none"> <li>• CREATE</li> <li>• UPDATE</li> </ul>
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: <ul style="list-style-type: none"> <li>• You cannot change agentID</li> <li>• If you leave the field blank, the userName must reference an existing agent</li> </ul>
userName	yes	Enter up to 255 characters as the username. Supports all characters, 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 (<>), 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 <i>Minimum Password Length</i> has been set in <b>Call Settings &gt; Miscellaneous</b> (see <a href="#">Global, on page 215</a> ).
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.
agentStateTrace	no	Indicates whether agent state trace is enabled for this agent. Defaults to False.

Field	Required?	Description
agentDeskSettingsName	no	<p>Enter the desk settings associated with this agent.</p> <p>In a CREATE operation, your entry of agentDeskSettingsName generates an error when there is no desk settings with that name.</p> <p>Leaving this blank applies the System Default Desk Settings.</p>
agentTeamName	no	<p>Enter the team in which this agent is a member.</p> <p>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.</p>
skillgroup(s)	no	<p>Enter the skill groups with which this agent is associated, delimited by the ";" character. For example: sales;billing;support.</p> <p>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.</p>
defaultSkillGroup	no	<p>Enter the default skill group associated with this agent. If the field is specified, it must reference a skill group defined for the agent.</p> <p>In an UPDATE operation, an error is generated if the value is no longer one of the agent's skill groups.</p>
attributes	no	<p>These fields are name = value pairs delimited by the ";" character, where = value is optional for existing attributes. For example, english=true;sales=7.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>To clear an agent's attribute value and reestablish the attribute default on a bulk update, just specify the attribute name, for example, english.</p> <p>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.</p>



Field	Required?	Description
supervisor	no	Indicates whether the agent is a supervisor. Defaults to False.
supervisorTeams	no	<p>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.</p> <p>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.</p>
siteName	no	<p><b>Note</b> This field is mandatory for Packaged CCE 4000 agent and 12000 agent deployments.</p> <p>The site name for this dialed number.</p> <p>For remote sites, the value must match an existing remote site name.</p> <p>For the main site, do not specify any value.</p>
ecePerson	no	Indicates whether the agent is a ECE enabled. Defaults to False.
screenName	yes, if ecePerson is entered	
emailAddress	no	<p>The email address of the agent. Maximum length is 50 characters.</p> <p>The following must be true for any email address:</p> <ul style="list-style-type: none"> <li>• Must include only one @ character.</li> <li>• Must include at least one character between @ and dot ( . ).</li> <li>• Must include one dot (.) after @ character.</li> <li>• Dot (.) must not be the last character.</li> </ul> <p><b>Note</b> Characters like round bracket ( ), angular bracket &lt; &gt; , and double quote " should not be included in the email address.</p>
digitalChannel	no	<p>Indicates whether the agent is enabled for digital channel interaction.</p> <p>Email address is mandatory when digitalChannel is set to True.</p> <p>The valid values are True or False. The default is False.</p> <p><b>Note</b> To set the value as True, make sure that you have added Cloud Connect in your inventory and you have registered it in the Control Hub. For more information, see <a href="https://help.webex.com/en-us/article/n24wo0fb/Register-Cloud-Connect">https://help.webex.com/en-us/article/n24wo0fb/Register-Cloud-Connect</a></p>

Field	Required?	Description
peripheralSetName	yes	<p><b>Note</b> This mandatory field is available only for Packaged CCE 4000 agent and 12000 agent deployments.</p> <p>The peripheral set name for this agent.</p> <p>The value must match an existing peripheral set name configured for the site specified in the siteName column.</p> <p>In an UPDATE operation, you cannot change peripheralSetName.</p> <p>In a DELETE operation, you cannot delete peripheralSetName.</p>

**Related Topics**

[Content File Rules](#), on page 245

**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	<p>Enter one of the following (case-insensitive):</p> <ul style="list-style-type: none"> <li>• CREATE</li> <li>• UPDATE</li> <li>• DELETE</li> </ul>
dialedNumberString	yes	<p>The dialedNumberString for this dialed number.</p> <p>Enter a string value that is unique for that routing type.</p> <p>Enter a maximum of 24 characters for Post Call Survey (PCS) routing types. For the External Voice routing type, enter a maximum of 24 characters if you are also entering the <b>Ringtone Media File</b> (optional) field. If you are not filling the <b>Ringtone Media File</b> field, enter a maximum of 25 characters. For all other routing types, enter a maximum of 25 characters.</p> <p>Valid values are alphanumeric, +, and @.</p> <p><b>Note</b> You cannot update dialedNumberString.</p>

Field	Required?	Description
routingType	yes	<p>The routing type for this dialed number. Values are 1 to 7.</p> <ul style="list-style-type: none"> <li>• 1 (External Voice): Dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP).</li> <li>• 2 (Internal Voice): Dialed number strings that can be called from a Cisco Unified Communications Manager phone.</li> <li>• 3 (Outbound Voice): Dialed number strings that are used by the Cisco Outbound Option Dialer.</li> <li>• 4 (Multichannel 1). Requests that come from Enterprise Chat and Email, Customer Collaboration Platform, or third party.</li> <li>• 5 (Multichannel 2). Requests that come from Enterprise Chat and Email, Customer Collaboration Platform, or third party.</li> <li>• 6 (Multichannel 3). Requests that come from Enterprise Chat and Email, Customer Collaboration Platform, or third party.</li> <li>• 7 (Post Call Survey). Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP).</li> </ul> <p>Multichannel routing types are available only if you have configured the peripherals for Enterprise Chat and Email, Customer Collaboration Platform, and/or Third Party Multichannel using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory.</p> <p>The order in which peripherals for these machines appear on the <b>Peripheral Gateways</b> tab (<b>Overview &gt; Infrastructure Settings &gt; Peripheral Gateways</b>), determines the routingType number (4, 5, or 6) for the machine. For example, if Customer Collaboration Platform peripheral appears first on the tab, it is routingType 4.</p> <p>See the <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html">https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html</a> for information about configuring the peripherals using Peripheral Gateway Setup.</p>
description	no	<p>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.</p>

Field	Required?	Description
callTypeName	no	<p>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.</p> <p>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.</p>
mediaRoutingDomainName	yes, for routingType 4, 5, and 6	<p>Optional for routingTypes 1, 2, and 3. If supplied, must be Cisco_Voice.</p> <p>Required for routingTypes 4, 5, and 6. The value must be Cisco_Voice or match an existing Media Routing Domain name.</p>
departmentName	no	<p>The department for this dialed number.</p> <p>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.</p> <p>If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.</p>
siteName	no	<p>The site name for this dialed number.</p> <p>For remote sites, the value must match an existing remote site name.</p> <p>For the main site, do not specify any value.</p>
ringtoneMediaFileName	no	<p><b>Note</b> Use this field when the routing type is External Voice.</p> <p>Enter the custom ringtone filename. Enter a maximum of 255 characters without any spaces.</p>
pcsEnabledDialedNumberPatterns	no	<p><b>Note</b> Use this field when the routing type is Post Call Survey.</p> <p>Enter Post Call Survey dialed number in the dialedNumberString field.</p> <p>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.</p>

**Related Topics**

[Content File Rules](#), on page 245

[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	<p>Enter one of the following (case-insensitive):</p> <ul style="list-style-type: none"> <li>• CREATE</li> <li>• UPDATE</li> <li>• DELETE</li> </ul>
dialedNumberString	yes	<p>The dialedNumberString for this dialed number.</p> <p>Enter a string value that is unique for that routing type.</p> <p>Enter a maximum of 24 characters for Post Call Survey (PCS) routing types. For the External Voice routing type, enter a maximum of 24 characters if you are also entering the <b>Ringtone Media File</b> (optional) field. If you are not filling the <b>Ringtone Media File</b> field, enter a maximum of 25 characters. For all other routing types, enter a maximum of 25 characters.</p> <p>Valid values are alphanumeric, +, and @.</p> <p><b>Note</b> You cannot update dialedNumberString.</p>

Field	Required?	Description
routingType	yes	<p>The routing type for this dialed number. Values are 1 to 7.</p> <ul style="list-style-type: none"> <li>• 1 (External Voice): Dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP).</li> <li>• 2 (Internal Voice): Dialed number strings that can be called from a Cisco Unified Communications Manager phone.</li> <li>• 3 (Outbound Voice): Dialed number strings that are used by the Cisco Outbound Option Dialer.</li> <li>• 4 (Multichannel 1). Requests that come from Enterprise Chat and Email, Customer Collaboration Platform, or third party.</li> <li>• 5 (Multichannel 2). Requests that come from Enterprise Chat and Email, Customer Collaboration Platform, or third party.</li> <li>• 6 (Multichannel 3). Requests that come from Enterprise Chat and Email, Customer Collaboration Platform, or third party.</li> <li>• 7 (Post Call Survey). Post Call Survey dialed number strings that apply to voice calls coming from Cisco Unified Customer Voice Portal (CVP).</li> </ul> <p>Multichannel routing types are available only if you have configured the peripherals for Enterprise Chat and Email, Customer Collaboration Platform, and/or Third Party Multichannel using Peripheral Gateway Setup tool, and added external multichannel machines to the System Inventory.</p> <p>To determine the routingType number (4, 5, or 6) for each peripheral, see the chapter <i>Routing Type API</i> in the <i>Cisco Packaged Contact Center Enterprise Developer Reference</i> at <a href="https://d1nmyq4gcgsfi5.cloudfront.net/site/packaged-contact-center/documentation/">https://d1nmyq4gcgsfi5.cloudfront.net/site/packaged-contact-center/documentation/</a>.</p> <p>See the <i>Cisco Packaged Contact Center Enterprise Features Guide</i> at <a href="https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html">https://www.cisco.com/c/en/us/support/customer-collaboration/packaged-contact-center-enterprise/tsd-products-support-series-home.html</a> for information about configuring the peripherals using Peripheral Gateway Setup.</p>
description	no	<p>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.</p>

Field	Required?	Description
callTypeName	no	<p>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.</p> <p>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.</p>
mediaRoutingDomainName	yes, for routingType 4, 5, and 6	<p>Optional for routingTypes 1, 2, and 3. If supplied, must be Cisco_Voice.</p> <p>Required for routingTypes 4, 5, and 6. The value must be Cisco_Voice or match an existing Media Routing Domain name.</p>
departmentName	no	<p>The department for this dialed number.</p> <p>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.</p> <p>If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.</p>
siteName	no	<p><b>Note</b> This field is mandatory.</p> <p>The site name for this dialed number.</p> <p>For remote sites, the value must match an existing remote site name.</p> <p>For the main site, do not specify any value.</p>
ringtoneMediaFileName	no	<p><b>Note</b> Use this field when the routing type is External Voice.</p> <p>Enter the custom ringtone filename. Enter a maximum of 255 characters without any spaces.</p>
pcsEnabledDialedNumberPatterns	no	<p><b>Note</b> Use this field when the routing type is Post Call Survey.</p> <p>Enter Post Call Survey dialed number in the dialedNumberString field.</p> <p>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.</p>

Field	Required?	Description
peripheralSetName	yes	<p><b>Note</b> This field is mandatory.</p> <p>The peripheral set name for this dialed number.</p> <p>The value must match an existing peripheral set name configured for the site specified in the siteName column.</p> <p>In an UPDATE operation, you cannot change peripheralSetName.</p> <p>In a DELETE operation, you cannot delete peripheralSetName.</p>

### Bulk Call Type Content File

The content file for the call type bulk job contains these fields:

Field	Required?	Description
operation	yes	<p>Enter one of the following (case-insensitive):</p> <ul style="list-style-type: none"> <li>• CREATE</li> <li>• UPDATE</li> <li>• DELETE</li> </ul>
name	yes	<p>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.</p>
description	no	<p>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.</p>
serviceLevelThreshold	no	<p>Maximum time in seconds that a caller should wait before being connected with an agent.</p> <p>Enter a value in seconds, using positive 32-bit integers only.</p>
serviceLevelType	no	<p>Indicates how the system calculates the service level:</p> <ul style="list-style-type: none"> <li>• 1 = Ignore Abandoned Calls</li> <li>• 2 = Abandoned Calls have Negative Impact</li> <li>• 3= Abandoned Calls have Positive Impact</li> </ul> <p>If not specified, this field is set to the system default.</p>
bucketIntervalName	no	<p>Identifier of the bucket interval, used for reporting.</p> <p>If specified, the value must match an existing bucket interval.</p> <p>If not specified, this field is set to the system default.</p>



Field	Required?	Description
departmentName	no	<p>The department for this call type.</p> <p>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.</p> <p>If the department already exists, then that department can be entered by a global administrator or by an administrator who administers that department.</p>

**Related Topics**

[Content File Rules](#), on page 245

**Bulk Skill Group Content File**

The content file for the skill group bulk job contains these fields:

Field	Required?	Description
operation	yes	<p>Enter one of the following (case-insensitive):</p> <ul style="list-style-type: none"> <li>• CREATE</li> <li>• UPDATE</li> <li>• DELETE</li> </ul>
name	yes	<p>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.</p>
description	no	<p>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.</p>
serviceLevelThreshold	no	<p>Maximum time in seconds that a caller should wait before being connected with an agent.</p> <p>Enter a value in seconds, using positive 32-bit integers only.</p>
serviceLevelType	no	<p>Indicates how the system calculates the service level:</p> <ul style="list-style-type: none"> <li>• 1 = Ignore Abandoned Calls</li> <li>• 2 = Abandoned Calls have Negative Impact</li> <li>• 3 = Abandoned Calls have Positive Impact</li> </ul> <p>If not specified, this field is set to the system default.</p>

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	<b>Note</b> This field is mandatory for Packaged CCE 4000 agent and 12000 agent deployments. The site name for this dialed number. For remote sites, the value must match an existing remote site name. For the main site, do not specify any value.
peripheralSetName	yes	<b>Note</b> This mandatory 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 245

## Add and Maintain Bulk Jobs

- 
- 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: <ul style="list-style-type: none"> <li>• <b>Queued:</b> 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.</li> <li>• <b>Processing:</b> The bulk job is being processed. To view the progress, click <b>Log File Download</b> to monitor the log file.</li> <li>• <b>Succeeded:</b> All operations in the bulk job were successful.</li> <li>• <b>Partially Succeeded:</b> Some operations were successful, and some were unsuccessful.</li> <li>• <b>Failed:</b> All operations were unsuccessful.</li> <li>• <b>Cancelled:</b> A bulk job is canceled when the preceding bulk job is terminated due to unrecoverable error while this job was in the queued state.</li> </ul>
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.

Field	Description
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 <b>Download</b> 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	<p>Click <b>Download</b> 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.</p> <p>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.</p>

# Capacity

## Capacity Info

In **Unified CCE Administration**, click **Capacity** in the left navigation menu to see a table that provides following system capacity information:

<b>Column</b>	<b>Description</b>
<b>Status</b>	The status column shows where your system stands with respect to the capacity limit. The status icons are: <ul style="list-style-type: none"><li>• Green for 0-75% of capacity.</li><li>• Yellow for 76-95%.</li><li>• Orange for 96-99%.</li><li>• Red for when you are at 100%.</li></ul>
<b>Number of Configured</b>	Shows the name of the object.
<b>At Most</b>	Shows the maximum capacity of each configurable object that is allowed.
<b>Actual</b>	Shows the number of objects currently configured on your system.
<b>% Used</b>	Shows the percentage of the maximum capacity represented by your configuration.

