Contact Center as a Service

Admin Help - Tenant

Contents

1: Intro

This Help is for CCaaS tenant administrators of a contact center who configure and manage their tenant properties and tenant resources.

In the tenant help, the CCaaS UI for Agents and Supervisors is called CCaaS UI.

What's new

Log in using Unified Admin — Unified Admin is a portal application for tenant administrators that presents the administration applications you are allowed to access.

Log out — if you logged in using Unified Admin, when you click **Logout** in CCaaS Admin, the **App Selector** page appears.

Manage Personnel properties — added **Allowed Admin applications**.

Manage mailboxes — if the Tenant Encryption Key does not exist, the password cannot be saved or edited.

Legal disclaimer

This document is governed by the terms of the software license agreement and applicable contract (including addendums) entered into with Enghouse.

Support

To submit comments or questions about the information in this guide, please open a case with Enghouse Support.

2: Overview

This section contains the following topics:

- Log in
- Log in using Unified Admin
- Select the language
- Reseller view
- Tenant view
- Navigation pane
- List view
- Card view
- Item properties
- How to search
- How to filter
- How to use wildcards
- Multiple administrators
- Change your password
- Log out

Log in

See also Log in using Unified Admin.

The log in process is slightly different depending on the URL you use for CCaaS Admin and the identity provider configured by your administrator.

> **Note**
>
> - Reseller administrators can log on to multiple tenants.
> - Admin users can open several tabs in the same browser with one login.
> - If you log in again after your CCaaS application session becomes invalid, and while your ADFS or EIS provider's session is still valid, you do not need to type your password.

1. In your browser, in the **Address** bar, type the URL supplied by your supervisor or administrator, and then click **Go** or press **Enter**. The **Welcome to CCaaS Admin** page briefly appears.
   If you are already logged in, the main **CCaaS Admin** page will appear.

   > **Note**
   >
   > If you previously logged in using Unified Admin, the  **App Selector** button appears at the top left of the main **CCSP UI Admin** page.

2. If you are not already logged in:

   - If you are using the general application URL, for example, *https://ccsp1.pj16.loc/Admin*, the **Welcome to CCaaS** page will appear. Type your **Username** in User Principal Name (UPN) format, for example, *someone@domainname.com*, and click **Continue.**
   - If you are using the tenant's direct login URL, for example, *https://ccsp1.pj16.loc/portal/t1/Admin*, you do not see this page. Instead, go straight to step 3.

3. The next step depends on the identity provider configured by your administrator:

   - For Auth Server, if it is not already present, type your **Username** in User Principal Name (UPN) format, for example, *someone@domainname.com*. Type your **Password** and click **Log in**. The main **CCaaS Admin** page appears. If necessary, see Password expired message below.

     Alternatively:

     - If you are using the general application URL and your system is set up with an identity provider, click **Login with your identity provider**.
     - To change the username, click **Change user** to go to the **Welcome to CCaaS** page.

   - For ADFS, you are redirected to the ADFS login page to authenticate. Please consult your local procedures for how to proceed from this point.
   - For Enghouse Identity Server (EIS), you are redirected to the EIS login page. Type your **Password** and click **Log in**. The main **CCaaS Admin** page appears.

4. If necessary, see Additional login messages below.

Next, see Reseller view or Tenant view.

Password expired message

For Auth Server, if your password has expired or your administrator has set your account to require a password change at the next login, the next time you enter your password on the **Welcome to CCaaS** page, the **Password expired** notification appears.

1. In the notification, click **Change password**. The **Change password** dialog appears.
2. In **Old password**, type your current password.
3. In **New password**, type your new password. Do not use the double quote (") character or spaces.
4. In **Confirm password**, type your new password again.
5. Click **OK**.

Additional login messages

The following messages may appear when you try to log in:

- *Failed to get authorization for Admin use*. Your user profile is not permitted to use the CCaaS Admin application. Only landlord, reseller, and tenant administrators are permitted to use the CCaaS Admin application.
- *You are not authorized to view this page.* This can occur because:
  - You are logged in to an external identity provider with a different username than the one you entered on the **Welcome to CCaaS** page to log in to the CCaaS client application.
  - You entered a username on the **Welcome to CCaaS** page and were redirected to an external identity provider, where you log on with a different username.
- *Auth Server is not available or there is a misconfiguration*. You must contact your administrator. You will not be able to log in to CCaaS Admin until the issue is resolved.

Log in using Unified Admin

See also Log in.

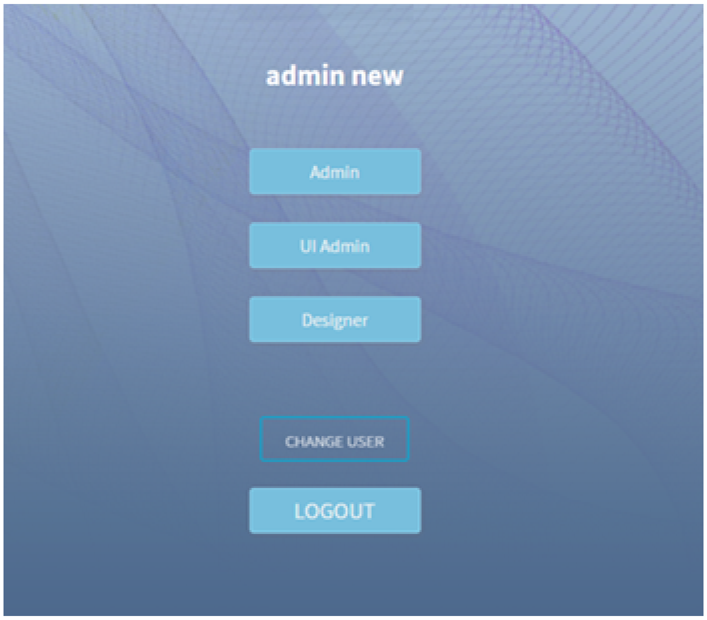
Unified Admin is a portal application for tenant administrators that presents the administration applications you are allowed to access.

> **Note**
> If you are allowed to access only one administration application, you go straight into that application without seeing the **App Selector** page.

1. If you are not already logged in:
   - If you are using the general application URL, for example, *https://ccsp1.pj16.loc/AuthServer/Pages/AppSelector.aspx*, the **Welcome to CCaaS** page will appear. Type your **Username** in User Principal Name (UPN) format, for example, *someone@domainname.com*, and click **Continue.**
   - If you are using the tenant's direct login URL, for example, *https://ccsp1.pj16.loc/portal/t1/apps*, you do not see this page. Instead, go straight to step 2.
2. The next step depends on the identity provider configured by your administrator:
   - For Auth Server, if it is not already present, type your **Username** in User Principal Name (UPN) format, for example, *someone@domainname.com*. Type your **Password** and click **Log in**. The **App Selector** page displays buttons for the administration applications you are allowed to access.

     If necessary, see Password expired message or Additional login messages.

     Alternatively:
     - If you are using the general application URL and your system is set up with an identity provider, click **Login with your identity provider**.
     - To change the username, click **Change user** to go to the **Welcome to CCaaS** page.
   - For ADFS, you are redirected to the ADFS login page to authenticate. Please consult your local procedures for how to proceed from this point.
   - For Enghouse Identity Server (EIS), you are redirected to the EIS login page. Type your **Password** and click **Log in**. The **App Selector** page displays buttons for the administration applications you are allowed to access.

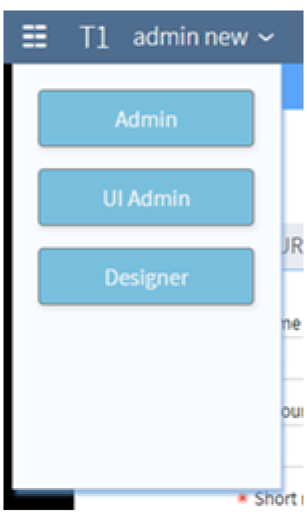


3. Click the **Admin** button. The main **CCaaS Admin** page appears.

Next, see Tenant view.

App selector menu

To open the other administration applications you are allowed to access, click  **App selector** at the top left of the main **CCaaS Admin** page, and then click the appropriate button.



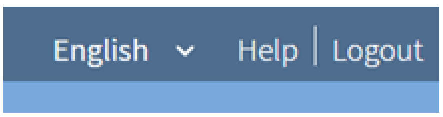
Each application opens in its own browser window. You can open several **CCaaS Admin** tabs in the same browser.

Select the language

Note

- By default, CCaaS Admin uses the language set in your browser. If the browser language is not available in CCaaS Admin, it uses the language configured by your administrator. If the configured language is not available in CCaaS Admin, it uses English.
- After you open CCaaS Admin, you can select to use one of the available languages. CCaaS Admin then automatically uses your selected language.

1. At the top right of the main CCaaS Admin page, click the language menu.



2. Select the language to use.

Reseller view

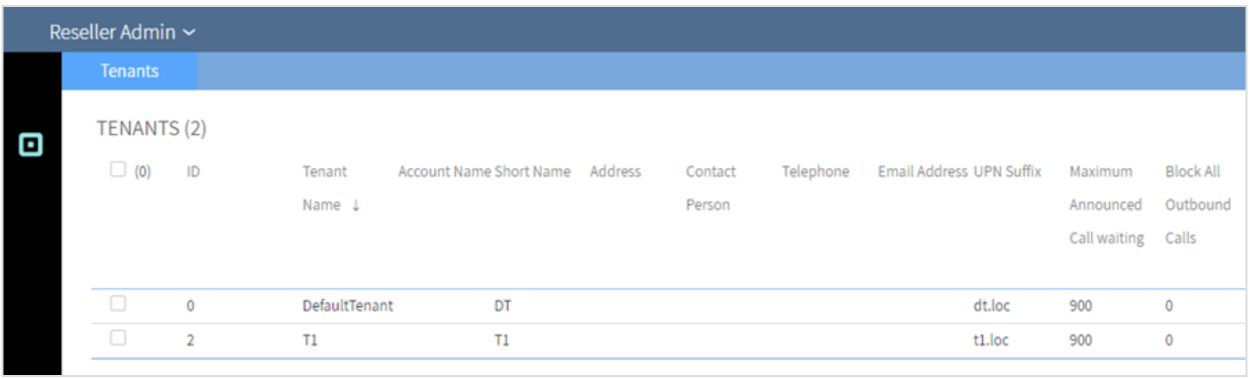
Select the tenant to manage

Return to the Tenants page

A reseller administrator is a tenant-wide administrator that performs tenant administrator tasks for the tenants that are assigned to them.

> **Caution**
> If no tenants are assigned to a reseller administrator, they can manage all tenants.

After logging in, reseller administrators see the **Tenants** page.



For navigation information, see List view.

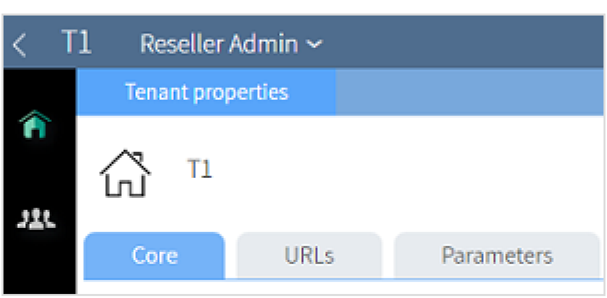
Select the tenant to manage

On the **Tenants** page, select the tenant to manage.

Next, see Tenant view.

Return to the Tenants page

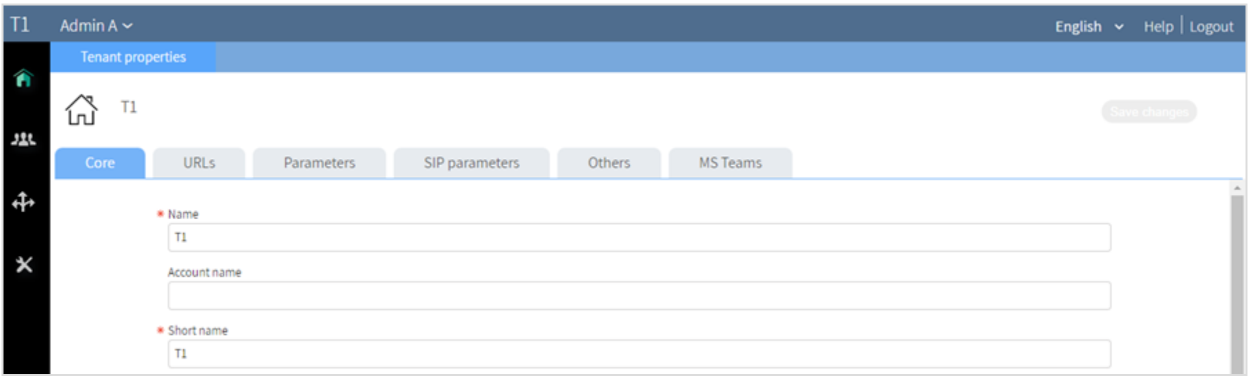
To return to the **Tenants** page, click the left arrow in the top left corner.



Tenant view

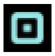
After logging in, tenant administrators see their Home page.

Some items can be viewed but not edited or deleted by tenant administrators. For details, see Configure tenant properties.



Navigation pane

Use the navigation pane as follows.

Icon	Description	Visible to reseller	Visible to tenant
	**Tenants** — click to select the tenant to manage.	Yes	No
	**Home page** — click to manage tenant properties.	Yes	Yes
	**Organization** — click to manage personnel (agents), groups, teams, permission profiles, skills, or SSO permission profiles.	Yes	Yes
	**Routing** — click to manage the DNIS pool, queues, folders, entry points, applications, release codes, or mailboxes.	Yes	Yes
	**Miscellaneous** — click to manage accounts, block codes, Dashboard views, interaction profiles, licenses (legacy), phone aliases, time zones, or wrap-up codes.	Yes	Yes

List view

Use the list view as follows.

To	Action
Add an item	Click .
Delete an item	Select the item's check box and then click .
Delete multiple items	Select multiple check boxes and then click .
Bulk assign agents to multiple skills or teams	Select multiple check boxes, click , and then click **Assign Agents to [item]**.
Clone agents, groups, queues, or skills	Select multiple check boxes, click , and then click **Clone [item]**.
Search for items	Type the criteria in the search box.
Sort	Click the column heading. The ↓ indicates the sort column and sort direction.
View the next page	Scroll to the end of the page.
View/edit an item	Click the item in the list to view/edit its properties in a dialog or, for tenants, personnel, and permission profiles, on tabs.
View counters	Total records appear in brackets after the resource name, for example, Teams (**5**). The number of: • Filtered records appear in brackets after the resource name, in front of the total records, for example, Teams (**2**/5). • Selected records appear in brackets at the top of the check box column, for example, (**1**).

Card view

Use the cards view as follows.

To	Action
Add an item	Click .
Delete an item	Select the item's check box and then click .
Delete multiple items	Select multiple check boxes and then click .
Hide the list	Click .
Search for items	Type the criteria in the search box. See How to search.
Sort	Click **Sort by**, select the field to sort by, and then click A-Z. The indicates the sort direction.
View the next page	Scroll to the end of the page.
View/edit an item	Click the item's card to view/edit its properties on tabs.
View counters	Total records appear in brackets after the resource name, for example, AGENTS (**29**). The number of: • Filtered records appear in brackets after the resource name, in front of the total records, for example, AGENTS (**5**/29). • Selected records appear in brackets at the top of the check box column, for example, (**3**).

Item properties

Mandatory fields

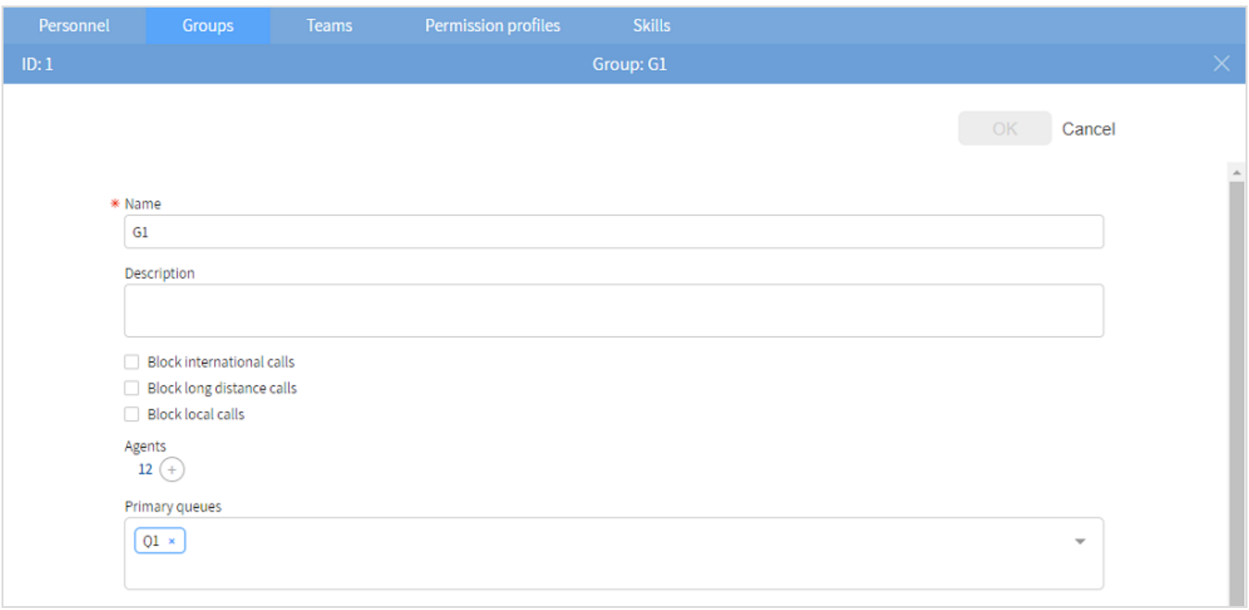
Error messages

Single item selection

Multiple item selection

After opening the relevant resource item list, click the particular item in the list to view/edit its properties in a dialog or, for tenants, personnel, and permission profiles, on tabs.

The following example shows the **Group: G1** dialog.

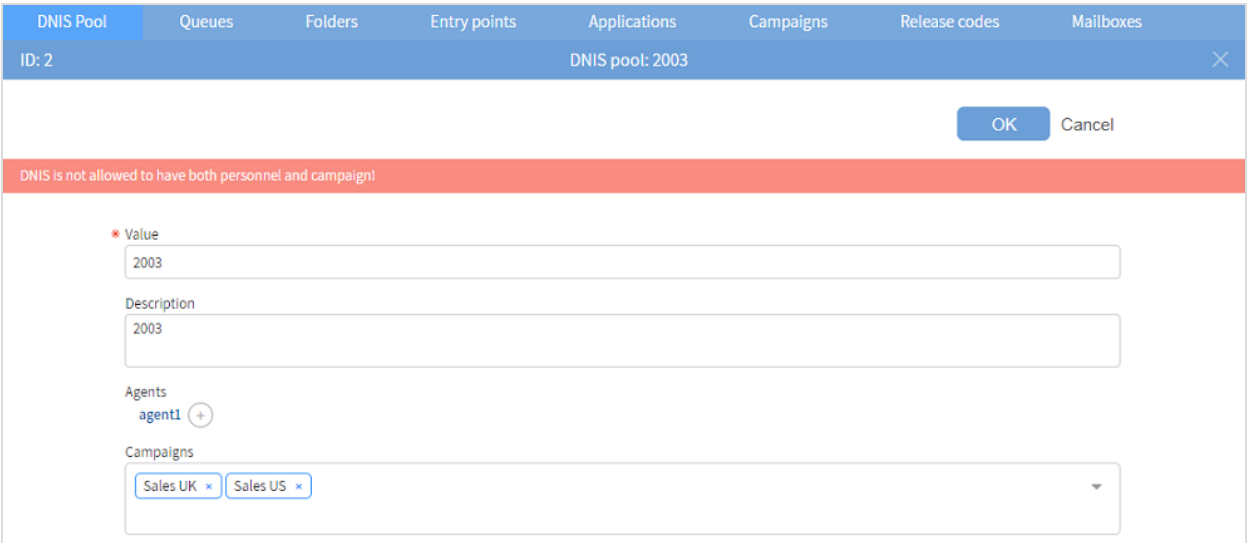


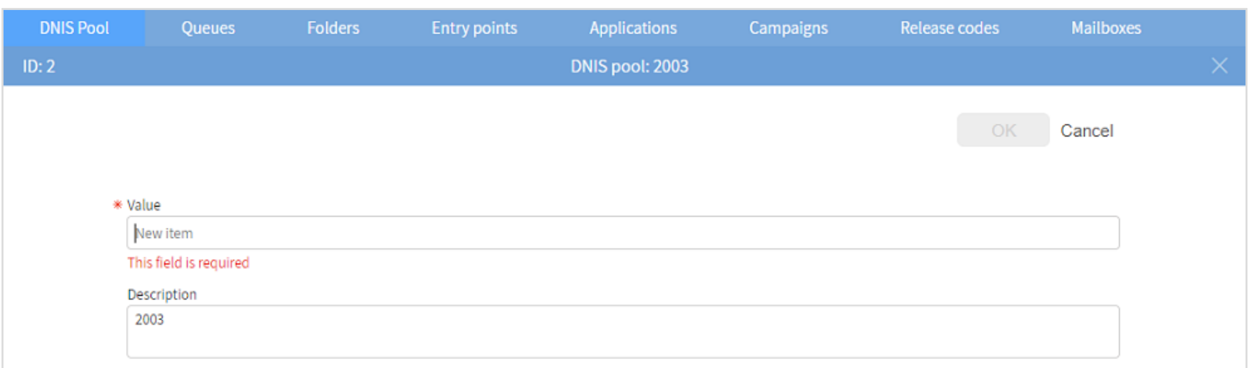
Mandatory fields

Mandatory fields are marked with a red asterisk (*).

Error messages

Error messages are displayed when you click **OK**, either at the top of the screen (error from server) or below the field (client validation).





Single item selection

To select a single item:

- Select the item by clicking it or pressing **Enter**.
- Search by typing the item's name.

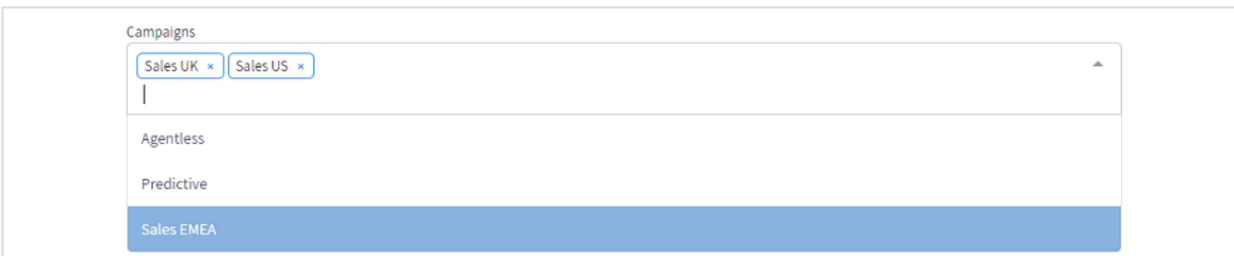
To remove a single item, unselect the item by clicking it or pressing **Enter**.

Multiple item selection

To select multiple items:

- Select each item by clicking it or pressing **Enter**. Each selected item appears in a bubble.
- Search by typing the item's name.

To remove multiple items, remove each item by clicking the **X** in its bubble.



When there are more than 50 items to select from and for agents,  appears next to the field.

Click  to open the **Choose items** dialog.

To select:

- A single item, click the row and then click **OK**.
- Multiple items, select the appropriate check boxes and then click **OK**.

To remove items, clear the appropriate check boxes and then click **OK**.

The counters show the total number of items, the number displayed, and the number selected. For details, see the counters in Lists.

How to search

Search generic lists

Search card-type lists

Search in the Choose items dialog

You can search for items in generic lists, card-type lists (Agents and Permission Profiles), and the Choose items dialog.

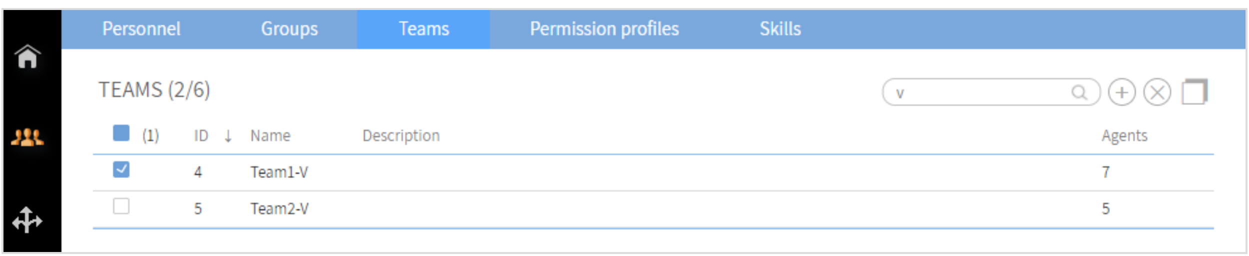
Each page shows up to 50 items and the total number of items appears in brackets, for example, AGENTS (210). When you search for items or sort the list by clicking the column heading, the total number of items are searched or re-ordered.

To view the next group of 50 items, scroll to the end of the page.

To search, type the search criteria in the search box. After 1 second of inactivity, the search starts automatically. You cannot type additional criteria while the search result is loading.

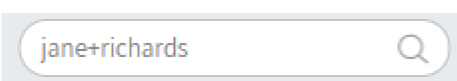
Search generic lists

The following example searches for teams that contain "V". The number of filtered teams that match the criteria appears in brackets, in front of the total, for example, Teams (**2**/6).

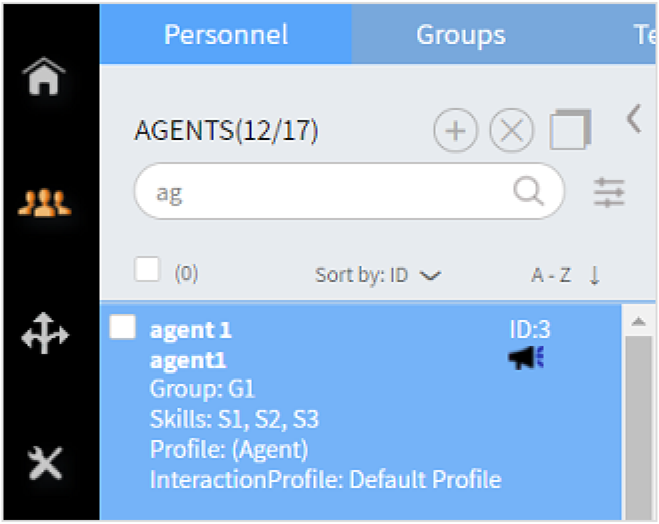


Search card-type lists

You can search for agents by their login ID, first name, last name, description, skills, or groups. To search by their full name, enter [first name]**+**[last name], for example:

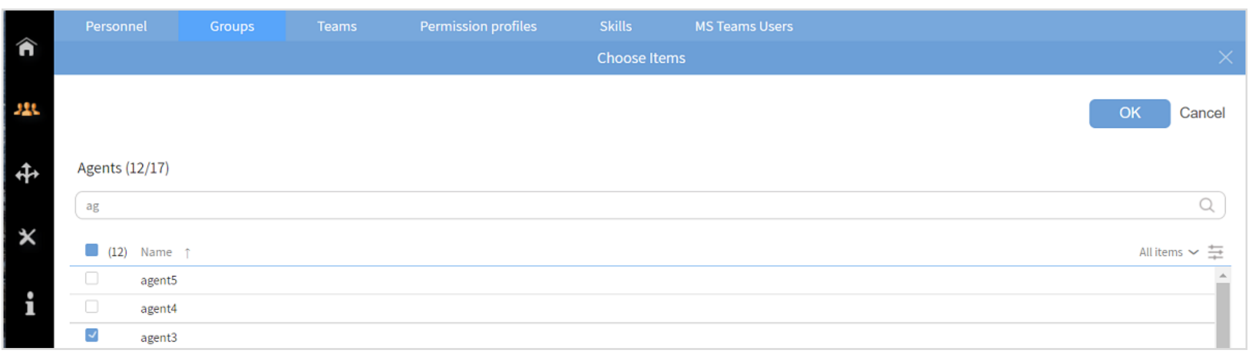


The following example searches for agents that contain "ag". The number of filtered agents that match the criteria appears in brackets, in front of the total, for example, AGENTS (**12/**17).



Search in the Choose items dialog

The following example searches for agent names that contain "ag".



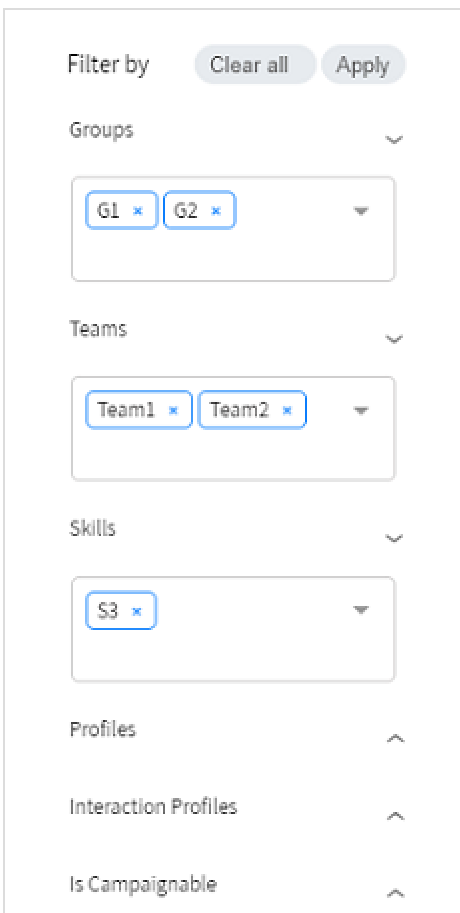
How to filter

Your permission profile determines which groups and teams you can filter by.

1. Click **Filter**.
2. In the **Filter by** dialog, select the criteria to filter by.

> **Note**
>
> - Groups, Teams, Skills, Profiles, Interaction Profiles, and IsCampaignable are AND conditions. The selected items inside each condition are OR conditions.
> - To restart the selection, click **Clear all**.
> - To close the **Filter by** dialog, click outside it.

   The following example filters for agents that are in Groups 1 or 2, AND in Teams 1 or 2, AND have the S3 skill.



3. Click **Apply**. The Active filter icon appears above the filtered list.

How to use wildcards

A common way to indicate a group of numbers that all have a similar pattern is by using wildcards.

If you have a series of numbers that all begin with 1**631940xxxx**, only the last four digits are different. To indicate this, you can use a question mark (?) to replace the digits which can vary. For example, **1631940????** can be used to represent 16319401234, 16319409890, or 16319403214.

The ? character can appear anywhere in a string. For example, **16319405?00** could represent 16319405000, 16319405100, 16319405200, 16319405300, 16319405400, 16319405500, 16319405600, 16319405700, 16319405800 or 16319405900.

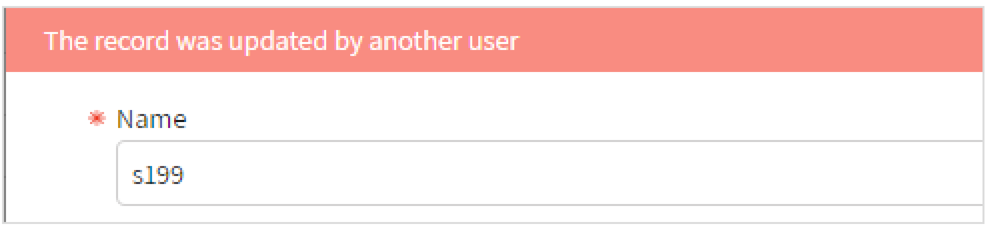
An asterisk (*) can be used to replace any combination of characters, in any quantity. For example, **1631940*** can be used to represent 16319401234, 16319409890, 16319401, 163194000000000.

Multiple administrators

Depending on how your contact center is configured, more than one administrator user may be logged on simultaneously.

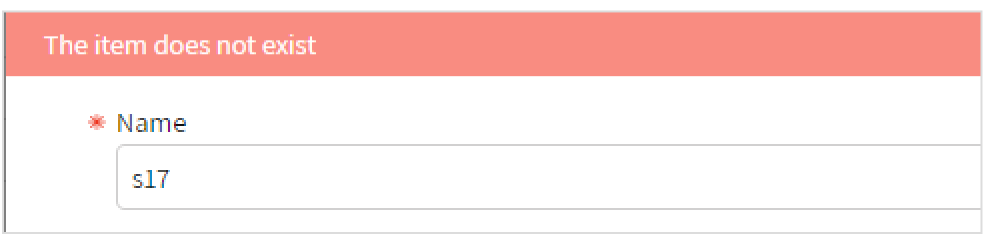
Simultaneous updates

If two administrator users open an item for update, the first user to click **OK** in the dialog succeeds with the update. When the other user clicks **OK**, the message *The record was updated by another user* appears in the dialog.



Simultaneous update and delete

If an administrator user opens an item for update, and another administrator user deletes the item, when the first user clicks **OK**, the message *The item does not exist* appears in the dialog.

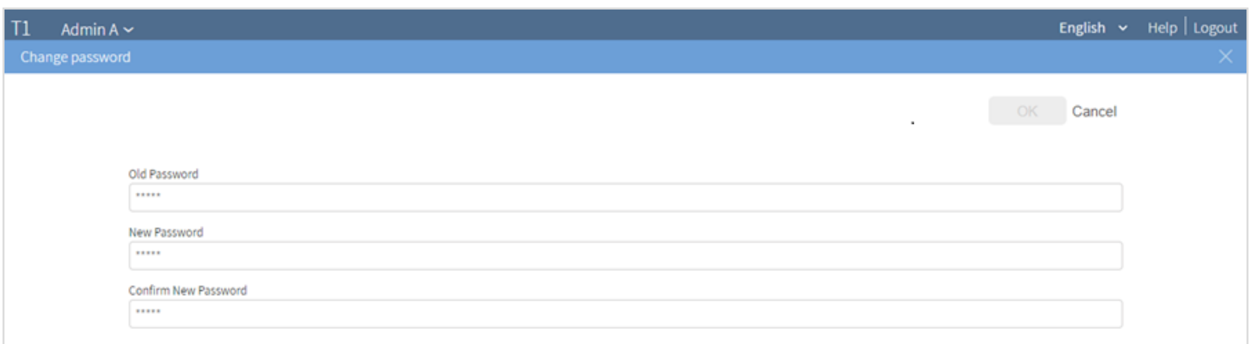


If an administrator user deletes an item, and another administrator user tries to update the item by clicking it in the list, the warning message *The item does not exist* appears.

Change your password

1. Log in to CCaaS Admin.
2. Click the down arrow after your user name and then click **Change User Password**.

3. In the **Change password** dialog, type your new password and confirm it. Do not use the double quote (") character or spaces.



4. Click **OK**.

Log out

> **Note**
>
> If you are using an external identity provider such as ADFS or EIS, when you click **Log out of your CCaaS session**, you are also logged out of your external identity provider.

1. At the top right of the main CCaaS Admin page, click **Logout**.
2. Do one of the following:
    - If you logged in directly, the **Logout** page appears:
        - If you want to return to CCaaS Admin, click **Log back in**.
        - If you have finished working with CCaaS, click **Log out of your CCaaS session**. The **Confirm logout** dialog appears. Click **Yes**. The following message appears: *You are now logged out of your session*.
    - If you logged in using Unified Admin, the **App Selector** page appears:
        - If you want to return to CCaaS Admin or use another administration application that you are allowed to access, click the appropriate button.
        - If you want to change the username, click **Change user** to go to the **Welcome to CCaaS** page.
        - If you have finished working with CCaaS, click **Logout**. The **Confirm end session** dialog appears. Click **Yes**. The following message appears: *You are now logged out of your session*.

Additional logout messages

When you click **Log out of your CCaaS session**, the following message may appear:

- *Logout was not completed successfully due to the Authentication Server being unavailable. Please contact your system administrator.*

1. Tell your system administrator about the issue and wait for it to be resolved.
2. When it is resolved, click **OK** to close the message dialog.
3. Click **Log out of your CCaaS** session again.

The application will return to the login page. Depending on the problem resolution, this may take slightly longer than normal.

Session expiry

Your CCaaS application session will become invalid when:

- The login session time exceeds the maximum CCaaS login session lifetime specified by your administrator.
- You log out of your CCaaS session using another application.
- You clear all cookies in the browser.

When your CCaaS application session becomes invalid, you must log in again. See Log in.

If you are logged in with an external identity provider (ADFS or EIS) and that provider’s login session lifetime exceeds the CCaaS login session lifetime:

- If you log in again using the general application URL, for example, *https://ccsp1.pj16.loc/Admin*, you need to enter only your username on the **Welcome to CCaaS** page, and are then automatically authenticated against your external identity provider.
- If you log in again using the tenant's direct login URL, for example, *https://ccsp1.pj16.loc/portal/t1/Admin*, you are automatically authenticated against your external identity provider and do not need to enter your username.

3: Configure tenant properties

You can configure the following tenant properties:

- Core
- URLS
- Parameters
- SIP parameters
- Others
- MS Teams

The landlord administrator adds the tenant and then completes all the required fields in the **Tenant Properties** dialog.

Tenants can view but not change the following properties:

- ID
- Name
- Account name
- Short name
- UPN suffix
- Trunk group
- All of the URLs
- All of the SIP parameters
- Integration of external media servers and selection of media server type

Tenants cannot change the properties shown as (landlord only) in this Help.

To configure tenant properties:

1. On the navigation pane, click **Home page.** The **Tenant Properties** page appears.
2. Edit or view the properties on the **Tenant Properties** page. The properties are arranged on the following tabs:
    - Core
    - URLS
    - Parameters
    - SIP parameters
    - Others
    - MS Teams
3. Click **Save changes**.

Manage core tenant properties

On the **Tenant Properties** page, on the **Core** tab, view/enter the following information:

- **Name** (required) — the name of the tenant. This name can be different from the **Account name**.
- **Account name** — the name to use for administration only. This value is case-sensitive.
- **Short name** (required) — the tenant's public folder name. The name should not contain any spaces, underscores, or special characters.
- **Address** — the tenant's billing address.
- **Contact person** — the main contact person's name.
- **Phone** — the main contact person's phone number or tenant's main number.
- **Email address** — the tenant's email address.
- **UPN suffix** (required) — the email and logon suffix for all users in the tenant's contact center.
- **Disable historical information for this tenant** — whether to disable logging of the tenant's call data to Historical Reports.
- **Outgoing and direct calls wrap-up timeout** (sec) — for how long to wait for agents to exit wrap-up before automatically timing out the wrap-up of an outdialed or a directly dialed incoming call. The default is 0 (no timeout).
- **Agent to agent call timeout** (sec) — for how long to wait for users to answer before automatically canceling an agent to agent call request. This value must be between 10-3600. The default is 30.
- **Call answered script timeout** (sec) — for how long to run the Call Answered Script. The script stops running when the timeout value is reached or when the agent hangs up the call. When set to 0, the agent that has been routed the call waits for the answer script to complete for as long as is needed. The agent can hang up the call while the call answer script runs, whether or not there is a timeout. The default is 0 (no timeout).
- **Enable call answered script for PD campaign** — whether to play the Call Answered Script for outbound dialing campaigns.
- **Media types** — the media types available to the tenant.

  > **Note**
  > CCaaS does not support calendar invites as a method of call delivery.

- **Aging timeout interval** (mins) — for messaging-related incoming calls:
  - For how long a deferred email/voicemail call waits for processing before the system reroutes the call
  - For how long the system waits before removing a call related either to a tenant that is unassigned from MS or an MS that is down. This allows grace time to assign another MS for a tenant or to wait for MS recovery after an unexpected failure.
  - The default is 480 minutes.

Manage tenant URLs

Landlord only can change these values.

On the **Tenant Properties** page, on the **URLs** tab, view/enter the following information:

- **Intelligent outdialing URL** — the URL used by the Dialing Plan:
  - For the advanced dial plan, set to *http://<servername>/AdvancedDialPlan/CheckPlan*
  - For the legacy dialing plan, set to *http://<servername>/DialingPlan/CheckPlan.asp*
- **Historical Reports URL** — the URL the tenant uses to access Historical Reports. This URL must be a Fully Qualified Domain Name (FQDN). For more information, see the *Enghouse CCaaS Historical Reports Help.*
- **RTR URL** — the URL the tenant uses to access Dashboard. This URL must be a FQDN and must end with a forward slash (/).

  > **Note**
  >
  > - The URL for Dashboard (2022) uses Dashboard instead of CosmoDashboard.
  > - To use the new Dashboard (2022) gadget with multiple browser support, append the option multibrowser to the Real Time Reports URL value, for example: *http://<servername>/Dashboard/?multibrowser*

- **CCSP Designer URL** — the URL used by the tenant to access the Designer application. This URL must be made available to all tenants.

  > **Note**
  >
  > In addition to the server that contains the Designer application, the tenant must have access to a server to which they can publish the CallXML scripts created in Designer. This server can be a hosted service of the system administrator, or on the tenant’s own server.

- **Replay URL** — the URL of the web server where interaction recordings for the tenant are posted. This URL must be the same URL established during installation.
- **Voicemail URL** — the URL the tenant uses to access voicemail. Set to *http://<servername>/designer/Scripts*
- **Elsbeth PowerContact server URL** — not enabled.

Manage tenant parameters

> **Note**
>
> CCaaS UI was previously called TouchPoint.

On the **Tenant Properties** page, on the **Parameters** tab, view/enter the following information:

- **Block agent-to-agent calls** — whether to prevent the tenant's agents calling one another.
- **Caller ID** — the identity the tenant chooses to present to a called party. This value can be text or a telephone number.

  > **Note**
  >
  > - Many called party phones can display only numeric information.
  > - Many countries prohibit insertion of erroneous information in this field.

- **Phone ANI** — the identifier used for call routing or billing. This is an optional field that can be required by your telephone carrier. ANI is different from Caller ID, but might be used by a telephone carrier to display caller identity to the called party. The value of this field is usually provided by the telephone company and is numeric text.
- **Maximum skill weight** — the maximum value for skill weighting. The default is 100.
- **CallData publishing mode** (required) — whether call data is published to the historical database at call arrival, call termination, or as soon as it is created (All). The default is Call arrival only.
- **Predictive dialing** — whether to allow outbound dialing campaigns.
- **Preview dialing** — whether to allow preview dialing.
- **Massive IVR dialing** — whether to allow IVR campaigns.
- **Block xfer/conf to agent** — whether to prevent the tenant's agents from transferring or conferencing calls to one another.
- **Impersonate CCaaS Connector** — whether to pass the user name and password to CCaaS Connector. If selected, the user name and password are passed to CCaaS Connector, which starts automatically if the agent has been logged on. If not selected, the user name and password are not passed to CCaaS Connector and the user has to log on again after logging on to CCaaS UI.
- **Block call/xfer to system** — whether to prevent the tenant from transferring calls to entry points, including returning calls to the IVR. For more information, see Manage entry points.
- **Agent list scope** (required) — the scope of the list from which agents select other agents for conferencing or call transfer. In the transfer dialog, CCaaS UI displays only team members for team specific scope and only group members for group specific scope. The default is Tenant-wide.
- **Hide agent names in RTR** — whether to replace agent names in real-time reports with random numbers. Used to comply with some regulations.
- **Inform agent when being monitored** — whether to display a message in CCaaS UI informing agents they are being monitored when supervisors start monitoring.

- **Reuse CSA media leg** — whether to allow the Circuit Switched Hybrid Agent (CSA) to put a call on hold without disengaging the call. If selected, the CSA can put a call on hold without disengaging the call. The CSA can be an agent using an external circuit switched telephone or external IP telephone. Requires that every VCS can communicate with any gateway in the system. If not selected, the VCS tears down the CosmoCall leg of the call.
- **Screen recording rate** (fps) (required) — how fast to capture agent screens. Greater capturing speed (bigger fps value) provides higher quality recordings, but requires more storage and may affect bandwidth requirements in extreme cases. The default is 1.
- **Screen recording quality** (%) (required) — deprecated.
- **Mailbox cleanup** (days) — how long to keep voicemail that is marked as read or deleted in the database. Agents can delete or keep voicemail that they have listened to. Deleted voicemail is marked as deleted in the recording database. Voicemail that was read but not deleted is marked as read. Unread voicemail is marked as new. Voicemail originates from the agents' direct telephone extensions. The default is 30.
- **Integration with external media servers** — whether to use the speech capabilities in Designer. If enabling, you must also select an **External media server type** (see below).
- **Email thread search mode** (required) — whether and how to search for email history. The options are:
  - **Automatic** — the feature is always available to the agents.
  - **On Demand** — an agent can turn on this feature when they need it. The advantage over Automatic is to save storage in the email database.
  - **Disabled** (default) — this feature is unavailable to agents.
- **External media server type** (required) — the protocol used with the external media server. The options are:
  - **None** (default)
  - **HP OCMP** — use for HP OCMP external media server.
  - **Generic MRCPv1** — sessions to the external media server are established using the RTSP protocol.
  - **Generic MRCPv2** — sessions to the external media server are established using the SIP protocol.
- **Dashboard SMTP server** — the SMTP server name or IP address for the DashboardEmailService to send email alerts from. Usually configured by the tenant administrator. The default is localhost.
- **Maximum call rejects** — the number of call reject occurrences for a call. The default is 0 (disabled).
- **Maximum pickup failures** — the number of pickup failure occurrences for a call. The default is 0 (disabled).
- **Max time allowed in queue before email call auto termination** (days) — the maximum time in the queue (between 0 and 30 days) before automatically terminating an email conversation. The default is 0 (disabled).
- **Action to take on MSR item when email call is auto terminated** (required) — whether to move the email item to the Rejected folder, move it to the Deleted folder, or delete it permanently. The default is Move to Rejected folder.
- **Max time allowed in queue before callback call auto termination** (days) — the maximum time in the queue (between 0 and 30 days) before automatically terminating a callback call. The default is is 0 (disabled).
- **Action to take on MSR item when callback call is auto terminated** (required) — whether to move the callback item to the Rejected folder, move it to the Deleted folder, or delete it permanently. The default is Move to Rejected folder.

- **Max time allowed in queue before voicemail call auto termination** (days) — the maximum time in the queue (between 0 and 30 days) before automatically terminating a voicemaill call. The default is is 0 (disabled).
- **Action to take on MSR item when voicemail call is auto terminated** (required) — whether to move the voicemail item to the Rejected folder, move it to the Deleted folder, or delete it permanently. The default is Move to Rejected folder.
- **Recording format** (required) — the recording format. The options are:
  - **GSM 6.10** (default) — the GSM mono recording is stored in the recording database.
  - **PCM 16 bit stereo** — the recording is converted into a stereo format and saved into the directory configured as the recording storage folder.
  - **Both** — the GSM mono recording is stored in the recording database and the stereo recording is saved into the directory configured as the recording storage folder.

  > **Note**
  > Stereo recording is not stored in the recording database and cannot be accessed using Replay.

- **Recording storage folder** — the target directory for all stereo format recordings. The default is blank.
- **Enable KCO setting** — whether to enable agents to remain connected to CCaaS through an alternative device for the duration of their shift.
- **SAML fingerprint** — the fingerprint that identifies the tenant.
- **Recording encryption public key** — the thumbprint of the tenant's public encryption key. The value can contain spaces or dashes.
- **Recording encryption key server URL** — the HTTPS URL of the key server web service, for example: *https://de-keyserv/keyserver/getkeys.aspx.*
- **Encryption enabled** — whether to enable encryption of recordings by the DTR servers.
- **Encrypted recording restrictions** (required) — the restrictions that apply to supervisors when playing back encrypted recordings. The default is Playback and save.

  > **Note**
  > The **Encrypted recording restrictions per agent** parameter value set in Personnel properties overrides this value, unless the Personnel properties value is set to None.

- **SBC IP address/hostname** — the IP Address or hostname of SBC used as bridge between Agent and VCS. Can be the address of the load balancer used to distribute connection over different SBC devices. To use hostname, the setting for the DNS machine used to resolve the entry must exist on the Agent local machine.
- **SBC plain transport port** — the port on the SBC to which connection is made from the Agent leg when SRTP is not used. The **Use SBC as proxy** parameter must be enabled. The default is 5060.
- **SBC secure transport port** — the port on the SBC to which connection is made from the Agent leg when SRTP is used. The default is 5061.
- **Use SBC as proxy** — whether to use SBC as the intermediate device between the Agent and VCS leg when SRTP is not used.
- **Use SRTP** — whether to use SRTP on the Agent leg. If SRTP is used, you don't need to select Use SBC as Proxy, but if both are selected, Use SRTP overrides Use SBC as Proxy.

> **Note**
>
> If **Use SRTP** is not select for the tenant but is selected for an agent, SRTP is used for that agent. See Manage personnel phone settings.

- **SRTP CA certificate name** — the file name of Central Authority certificate used to validate TLS connection from Agent to SBC, when calls are established. SRTP CA Certificate Name must be the same as the name of relevant certificate file added under Tenants Information. TLS 1.0 is supported for SIP negotiation between Agent and SBC.
- **Script log verbosity** (landlord only) (required) — the script log verbosity. The default is Inherited.
- **Script log traces** (landlord only) (required) — whether to use script log traces. The default is Inherited.
- **Tenant encryption key** — an ASCII string that is unique across the system. The maximum size is 512 characters.

> **Note**
>
> We recommend that you change this key occasionally to ensure mailbox security.

- **Tenant messaging folder purge interval** (hours.fraction) — not in use.
- **Audio file URL rebound other telco reject** — leave blank.
- **ClientUploadService process priority** (required) — the process priority for the client upload service that searches in the background for files to compress and upload. The service searches every 3 minutes and performs 1 compression at a time. The default is BelowNormal.

> **Note**
>
> The client upload service should have fewer resources than the screen recording process.

- **ClientUploadService process affinity** — the processors that are allowed to run the client upload service. The default is blank (use all processors).

> **Note**
>
> We recommend that you use all processors so compressing and uploading finishes as fast as possible. However, if you need to reserve processors for CCaaS UI, screen recording and other processes, you can set the client upload service processor affinity to use only half of the processors by configuring a list of even CPU numbers, separated by a comma, for example, 0,2,4,6

- **Screen recording process priority** (required) — the process priority for the screen recording service that captures the agent's screen during CCaaS UI calls. The default is Normal.

> **Note**
>
> The screen recording process should have more resources than the client upload service but we do not recommend a process priority bigger than normal because this can affect OS tasks.

- **Screen recording process affinity** — the processors that are allowed to run the screen recording service. The default is blank (use all processors).
- **Vidyo developer key** — an ASCII string provide by Enghouse Vidyo to link to the Vidyo service.
- **IVR root path** — the location of the published Designer scripts, for example, *\\ccsp1\ivr\t1*
- **Recording database location** — the location of the recording database. The options are:

    - **CCSP Recording Data Store** (default) — call records will be saved to the CCaaSRecording database.
    - **QMS Database** — call records will be sent to QMS only.
    - **Both** — call records will be saved to the CCSP Recording database and sent to QMS.
- **External IdP Type** (landlord only) — the external Identity Provider to use. The options are:
    - **None** (default) — use the CCaaS Auth Server to authenticate users.
    - **EIS** — use the Enghouse Identity Server to authenticate users.
    - **ADFS** — use Active Directory Federation Services to authenticate users.
- **External IdP Host URL** (landlord only) — the URL where the user's browser is redirected for authentication. Only relevant when the **External IdP Type** is not **None**.
- **External IdP Client ID** (landlord only) — the identifier by which the CCaaS Auth Server is known to the External Identity Provider. Only relevant when the **External IdP Type** is **EIS**.
- **External IdP Client Secret** (landlord only) — the allocated password that the CCaaS Auth Server must use when requesting authentication from the External Identity Provider. Only relevant when the **External IdP Type** is **EIS**.
- **Access Token Lifetime (min)** — the validity period in minutes of the access token received by the client application from the CCaaS Auth Server. The default is 15.
- **Refresh Token lifetime (min)** — the validity period in minutes of the refresh token received by the client application from the CCaaS Auth Server. The default is 600.
- **Login Session Lifetime (min)** — the duration of the CCaaS SSO login session in minutes. The default is 720.

Manage tenant SIP parameters

Landlord only can change these values.

On the **Tenant Properties** page, on the **SIP parameters** tab, view/enter the following information:

- **P-asserted-identity SIP** — the SIP equivalent of the ANI in SIP URI format. Telephone carriers use this information to identify authorized users, such as a particular tenant. This is not Caller ID and is not shown to the called party. CCaaS sends this information to the remote party in a SIP INVITE message. The telephone carrier provides this value.
- **P-asserted-identity TEL** — the phone number in TEL URI format. This information is similar to P-Asserted-Identity SIP but in telephone format and is sent in a SIP INVITE message.
- **Identity of transfer from IVR** — whether and how to transfer caller identity to the third party. Used only for calls transferred from IVR script (by using the Bridge and Transfer Designer blocks). The options are:
    - **Of the original call** (default) — ANI, PAI, and privacy transferred to the third party are copied from the original inbound leg of the call.
    - **Anonymous** — the third party does not receive the identity of the caller or the tenant.
    - **Of the tenant** — the third party of a transferred call receives the tenant's caller ID.
- **Identity of outgoing call** — whether and how to transfer the identity of the original caller to the called party. Used for calls transferred by agents or regular outgoing calls made by agents. The options are:
    - **Of the original call** (default) — if a call is transferred by agent, the identity of the original caller is transferred to the called party. For a regular outgoing call, the identity of the individual agent, if it is assigned, is transferred to the called party.
    - **Anonymous** — the identities of the original caller and the tenant are not disclosed.
    - **Of the tenant** — the called party receives the individual agent caller ID, if it is assigned.
- **When caller requests privacy** — whether to show caller identities to the tenant. Caller identity is usually stripped from a call by caller request even before the call arrives at CCaaS. For example, if the system is installed in an enterprise or in a service provider that is not a carrier, the setting has no effect on the system. If installed in the core of a carrier network, CCaaS may receive caller identities even if callers ask to hide it. The system administrator may decide to show caller identities to the tenant. This parameter is also used by H.323. The options are:
    - **Do not hide** (default) — pass the caller's identity and do not hide it. Ignore the caller's request.
    - **Hide from agent** — hide only from agents. The identity is available for scripts and reports.
    - **Hide everywhere** — hide everywhere. Calls where the caller asks to hide his identity appear as Anonymous for agents, scripts, and reports.
- **Relay display name** — whether to relay the display name to other call participants. The display name is a textual description of the caller, such as the person’s name. If the caller has requested privacy and caller ID appears as Anonymous, no display name is associated with the call, regardless of this setting.

Manage other tenant properties

Caution

We highly recommend that you enable **Use folder segregation**.

When folder segregation is disabled:

- The following folders are not visible to agents and regular supervisors:
  - Rejected Emails, Deleted Emails, Replied, Not Replied, Drafts, Outbox, Sent Items
  - Deleted Callbacks
  - Voicemail, Archived Voicemails, Rejected Voicemails, Deleted Voicemails
- Agents and regular supervisors can only see their own callbacks marked with "call-to-me" and their own personal (not shared) deferred emails/voicemails.

On the **Tenant Properties** page, on the **Others** tab, view/enter the following information:

- **Media devices** — the video communications devices available to the tenant. The devices support two or more end points to a conversation.
- **Default application** — the application to execute if no other application evaluates to TRUE. See Manage applications.
- **Default time zone** — the tenant's default time zone. See Manage time zones.
- **Voicemail DNIS** — the DNIS for the tenant to use for personal voicemail.
- **Trunk group** — the trunk group assigned to the tenant.
- **Use folder segregation** — whether to use the folder segregation feature that enables selective access to system folders for all agents and supervisors based on permissions. The default is disabled. See above Caution.

Manage tenant MS Teams parameters

If you have the Teams integration, on the **Tenant Properties** page, on the **MS Teams** tab, view/enter the following information:

- **TeamsTenantID** — the **Directory (tenant) ID** found in Azure Portal’s App registration overview screen.
- **TeamsClientID** — the **Application (client) ID** found in Azure Portal’s App registration overview screen.
- **CacheExpiration** — the cache that hold the search results from the Teams directory is periodically checked to clear its expired entries, at the frequency defined in this parameter.
- **ResponseLimit** — the maximum number of presences to return to the agent. Must be greater than zero. We recommend 50.
- **Polling** — whether to enable polling to get presences from the Teams Graph API. The default is disabled.
- **Polling interval** — the time in milliseconds between each request to get presences from the Teams Graph API.

4: Configure tenant resources

You can configure the following tenant resources:

- Accounts
- Applications
- Block codes
- Dashboard views
- DNIS pool
- Entry points
- Folders
- Groups
- Interaction profiles
- Legacy licenses
- Mailboxes
- Permission profiles
- Personnel
- Phone aliases
- Queues
- Release codes
- Skills
- SSO permissions
- Teams
- Time zones
- Wrap-up codes

Manage accounts

View the Accounts list

Add an account

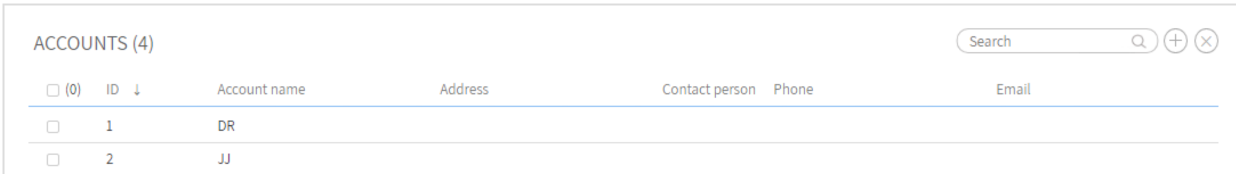
Edit an account

Delete an account

Accounts track individual call information. Calls are assigned to accounts via scripts. Account information can be used for billing and other purposes.

View the Accounts list

1. On the navigation pane, click **Miscellaneous.**
2. If necessary, click the **Accounts** tab. The **Accounts** list appears. For navigation information, see List view and How to search. For column descriptions, see Add an account.



Add an account

1. On the **Accounts** page, click **Add**. The **New Account** dialog appears.
2. Enter the following information:
    - **Account name** (required) — the name of the account.
    - **Address** — the mailing address.
    - **Contact person** — the name of the primary contact person for this account.
    - **Phone** — the primary contact's or the account's phone number.
    - **Email** — the primary contact's or the account's email address.
3. Click **OK**.

Edit an account

1. On the **Accounts** page, click the item to edit. The **Account: [Name]** dialog appears.
2. Edit the information. For details, see Add an account.
3. Click **OK**.

Delete an account

1. On the **Accounts** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage applications

Applications refers here to a set of scripts created using Designer that define a call flow. You can define multiple call flow applications. One of these applications is selected for each call.

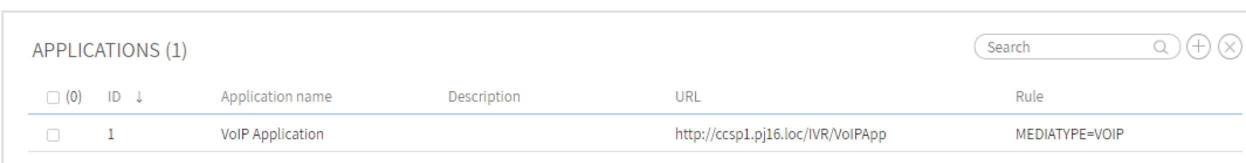
Before running a script, CCaaS applies a set of rules to determine which application to use. The rules are checked in the order in which they appear in CCaaS Admin, that is, in creation order. The first application whose rule evaluates to True is selected. If no rule evaluates to True, then CCaaS runs the default application.

The call preserves the last selected application ID that was used. However, this application ID is not preserved when an email or voicemail call is deferred or transferred to system (TTS). If the entry point for TTS has a configured application ID, then this application ID is preserved instead.

These rules use call parameters to determine which application to run. For voice calls, DNIS is used. For chat calls, the calling user URL is used, and for messaging calls the email folder name is used.

View the Applications list

1. On the navigation pane, click **Routing**.
2. Click the **Applications** tab. The **Applications** list appears. For navigation information, see List view and How to search. For column descriptions, see Add an application.



Add an application

1. On the **Applications** page, click **Add**. The **New Application** dialog appears.
2. Enter the following information:
    - **Application name** (required) — the name of the application.
    - **Description** — a description of the application and its use.

    - **URL** (required) — the URL where the Designer XML scripts are published.
    - **Rule** (required) — the rule to determine whether to select the application. See Creating rules below.

3. Click **OK**.

Creating rules

Rules are used to determine which application (script) is run when a call arrives in the contact center. A rule consists of a compilable VB script.

To select the application based on the call's media type, use one of the following logical comparison statements:

- MEDIATYPE=CALLBACK
- MEDIATYPE=VOICEMAIL
- MEDIATYPE=EMAIL
- MEDIATYPE=VOIP
- MEDIATYPE=CHAT

Below are some examples of rules.

```
DNIS = 6319404200 AND Now > CDate(""8/4/2017 6:54:10 PM""), CDate is a date constant.
```

```
CDate(""6:54:10 AM"") < Time And Time < CDate(""6:54:10 PM"")
```

```
Date > CDate(""8/4/2017"")
```

```
DNIS = 631* AND Date > CDate(""8/4/2017"")
```

When creating rules:

- **DNIS** must be used if you want to specify DNIS.
- **DNIS** is not supported when media type is CallBack or VoiceMail.
- **MAILFOLDER** represents the last ACD folder name.
- **MAILFOLDEREMAIL** represents the last ACD folder email address.
- **MAILFOLDER** and **MAILFOLDEREMAIL** in the same rule are not supported.
- **Now** means current date and time.
- **Time** represents the current time.
- **Date** represents the current date.
- **CDate** must have double quotation marks ("") on both sides of the rule.

For email messages rules, instead of **DNIS** specify **MAILFOLDER**.

```
MAILFOLDER = foldername And Date > CDate(""8/4/2017"")
```

For chat call rules, the Application Name can be specified on the web caller while making a chat call. If an Application Name is supplied in the web caller, and it matches one of the defined Application Names, that application (script) is run even though Application Rule doesn't evaluate to TRUE.

Note

- Wildcard matching is supported.
- If you want exceptions to run alternate scripts and everything else to run the default application, then the default application must be added last in CCaaS Admin since rules are processed in the order of creation. The default application is run if no other application rule evaluates to True.

Set the default application

1. On the navigation pane, click **Home page.** The **Tenant Properties** dialog appears.
2. Click the **Others** tab.
3. In **Default application**, select the application.
4. Click **Save changes**.

Edit an application

1. On the **Applications** page, click the item to edit. The **Application: [Name]** dialog appears.
2. Edit the information. For details, see Add an application.
3. Click **OK**.

Delete an application

1. On the **Applications** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage block codes

View the Block Codes list

Add a block code

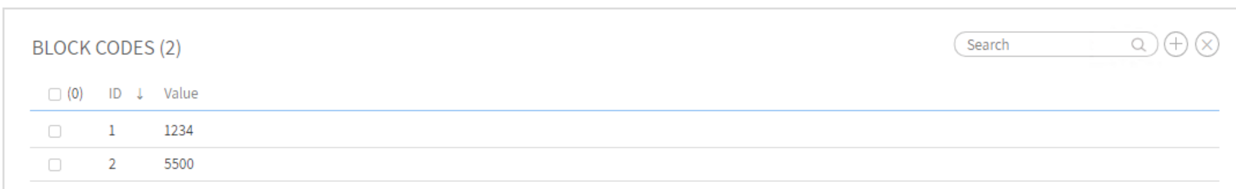
Edit a block code

Delete a block code

Block codes are used to block group or agent access to specific area codes that you select.

View the Block Codes list

1. On the navigation pane, click **Miscellaneous.**
2. Click the **Block Codes** tab. The **Block Codes** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a block code.



Add a block code

1. On the **Block Codes** page, click **Add**. The **New Block Code** dialog appears.
2. Enter the following information:
    - **Value** (required) — the code to block. This is generally an area code such as 900 or 888. To specify multiple block codes, enter their values separated by commas, for example, **888,999,800,45**.
    - **Groups** — select the groups to apply the block code to from the list.
    - **Agents** — click **Add items** and select the agents to apply the block code to from the list. See Filter for agents.
3. Click **OK**.

Edit a block code

1. On the **Block Codes** page, click the item to edit. The **Block Code: [Value]** dialog appears.
2. Edit the information. For details, see Add a block code.
3. Click **OK**.

Delete a block code

1. On the **Block Codes** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage Dashboard views

View the Dashboard Views list

Edit a Dashboard view

The initial name of a view is assigned by the user who created it in Dashboard. That user is the first owner and is the first to have sole permission to edit or delete the view.

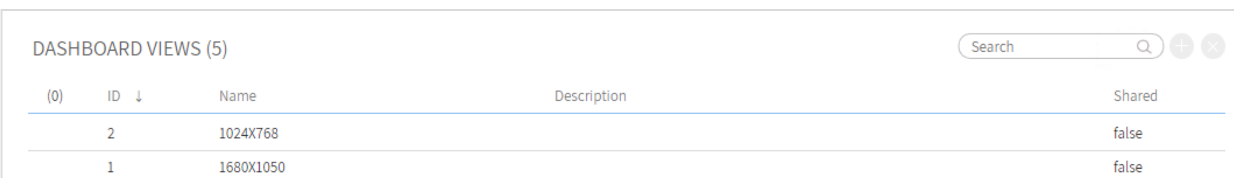
> **Note**
>
> In Dashboard, you can rename a view but you cannot change its owner.

In CCaaS Admin, you can:

- Rename a view — the new name will appear in the Dashboard window.
- Change the owner of a view — only the new owner can edit or delete the view.
- Allow other users to share a view.

View the Dashboard Views list

1. On the navigation pane, click **Miscellaneous.**
2. Click the **Dashboard Views** tab. The **Dashboard Views** list appears. For navigation information, see List view and How to search. For column descriptions, see Edit a Dashboard view.



Edit a Dashboard view

1. On the **Dashboard Views** page, click the item to edit. The **Dashboard View: [Name]** dialog appears.
2. Enter the following information:
   - **Name** (required) — the name of the view.
   - **Description** — a description of the view.
   - **Owner** — to re-assign the permission to edit the view, select a user with a supervisor profile.
   - **Shared** — whether to allow the view to be shared.
3. Click **OK**.

Manage the DNIS pool

> **Note**
> CCaaS UI was previously called TouchPoint.

View the DNIS Pool list

Add a DNIS pool

Assigning a DNIS pool

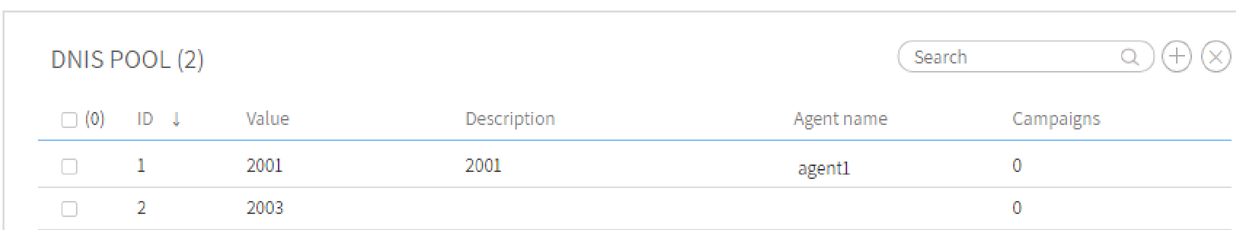
Delete a DNIS pool

The DNIS pool is added by the landlord administrator, who then allocates each DNIS to a tenant.

> **Note**
>
> - You can assign the DNIS to only one user.
> - Be sure to allocate a DID to an IP Phone user who has a permanent extension and does not use CCaaS UI.

View the DNIS Pool list

1. On the navigation pane, click **Routing**.
2. If necessary, click the **DNIS Pool** tab. The **DNIS Pool** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a DNIS pool and Assigning a DNIS pool. The Agent name column shows the agent the DNIS pool is assigned to. The Campaigns column show the number of campaigns the DNIS pool is assigned to.



Add a DNIS pool

Landlord only.

1. On the **DNIS Pools** page, click **Add**. The **New DNIS Pool** dialog appears.
2. Enter the following information:
   - **Value** (required) — the telephone number, local extension, URL, or any other appropriate DNIS identifier. The value can include wildcards. For details, see How to use wildcards. Separate DNISs with a

space, comma, or semicolon.

- **Description** — a description of the DNIS pool.

3. Click **OK**.

Assigning a DNIS pool

1. On the **DNIS Pool** page, click the item to edit. The **DNIS Pool: [Value]** dialog appears.
2. Enter the following information:
   - **Agents** — click **Add items** and select the agent to assign the DNIS to. See Filter for agents.
   - **Campaigns** — leave blank.
3. Click **OK**.

Delete a DNIS pool

Landlord only.

1. On the **DNIS Pools** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage entry points

> **Note**
> CCaaS UI was previously called TouchPoint.

[View the Entry Points list](#)

[Add an entry point](#)

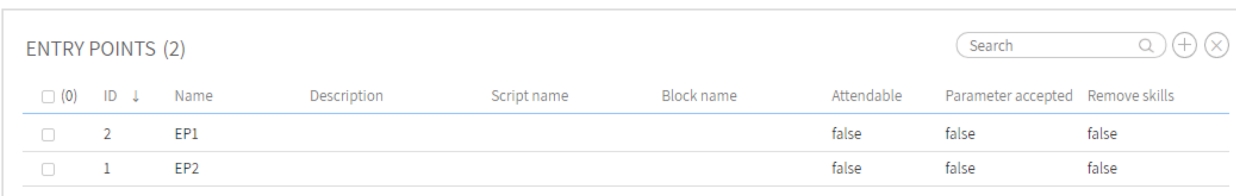
[Edit an entry point](#)

[Delete an entry point](#)

> **Caution**
> You must also create the script entry point in your scripts. Assign it the same name you assign in CCaaS Admin.

View the Entry Points list

1. On the navigation pane, click **Routing**.
2. Click the **Entry Points** tab. The **Entry Points** list appears. For navigation information, see List view and How to search. For column descriptions, see Add an entry point.



ENTRY POINTS (2)

(0)	ID	Name	Description	Script name	Block name	Attendable	Parameter accepted	Remove skills
	2	EP1				false	false	false
	1	EP2				false	false	false

Add an entry point

1. On the **Entry Points** page, click **Add**. The **New Entry Point** dialog appears.
2. Enter the following information:

   - **Name** (required) — the entry point name. This name appears in the user's **System** tab.
   - **Description** — a description of the entry point. This text appears as a tool tip in CCaaS UI.
   - **Queue** — to direct a call to a particular queue, select the queue. Only one queue can be assigned.
   - **Folder** — to place an email call in a particular folder, select the folder. Only one folder can be assigned.
   - **Application** — to assign the application to which the script in this entry point belongs, select the application. Only one application can be assigned.
   - **Script name** — the name of the script inside the application to execute when the agent selects this entry point. For example, to transfer to a point in the IVR script, type IVR.xml

- **Block name** — the name of the block inside the script where execution begins (optional). If omitted, execution starts from the **Start** block of the script.
- **Attendable** — whether you want the agent to choose whether to transfer or conference the call. If you want the agent only to transfer the caller to the entry point, clear the check box.

> **Note**
>
> Attendable entry points are not visible for email or chat calls.

- **Parameter accepted** — whether you want the parameter string of the Entry Point block to be passed to the script. Only one string can be passed.

> **Note**
>
> - If **Parameter accepted** is selected, the agent can type a value in the Parameter field of the CCaaS UI **System** tab.
> - To pass multiple parameters through the single string parameter, you can write a routine that passes the string in the script.

- **Remove skills** (voice only) — whether you want to remove skills from the original call when transferring to TTS.

> **Note**
>
> If the registry **RetainSkillsForTtsCall** exists on the relevant VCS, this setting is ignored unless the registry value is -1.

- **Groups** — if you want to limit the availability of the entry point to particular groups, select one or more groups. If no groups are selected, all agents can select this entry point.

3. Click **OK**.

Edit an entry point

1. On the **Entry Points** page, click the item to edit. The **Entry Points: [Name]** dialog appears.
2. Edit the information. For details, see Add an entry point.
3. Click **OK**.

Delete an entry point

1. On the **Entry Points** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage folders

View the Folders list

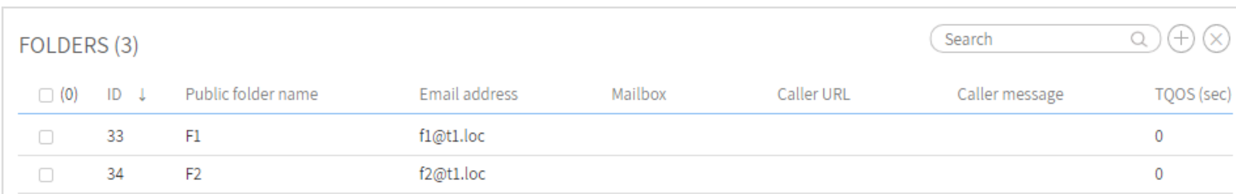
Add a folder

Edit a folder

Delete a folder

View the Folders list

1. On the navigation pane, click **Routing**.
2. Click the **Folders** tab. The **Folders** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a folder.



Add a folder

> **Note**
>
> The folder's **Email address** field must contain a valid email address. You must add any special folders that do not require an email address directly in the database.

1. On the **Folders** page, click **Add**. The **New Folder** dialog appears.
2. Enter the following information:

    - **Public folder name** (required) — the folder name. This name appears in Outlook under *Short Name/Public Folder Name*. This name must not contain spaces, underscores, or special characters. It cannot be named CallBack, Config, Dead-Letter, No-Reply, Outbox, Processed, or Reply because these are the names of hidden system folders.
    - **Email address** (required) — the email address of the folder. This address must not contain spaces, underscores, or special characters. The address can have a maximum of 64 characters before the at sign (@) and a maximum of 254 characters after it.
    - **Caller URL** — the URL to send with the email. This URL appears in the agent interface.
    - **Caller message** — the message to send with the email. This message appears in the agent interface.
    - **TQOS (sec)** — the amount of time in seconds in which an email call should be answered. TQoS can be used to specify levels of service for incoming calls.

- **Groups** — select the groups that have access to this folder.
- **Queue** — select the queue to assign to messages that arrive at this folder without a queue.
- **Skills** — select the skill requirements to assign to messages that arrive at this folder without a skill.

  > **Note**
  >
  > Skill settings can come from many sources, including the Folder and the Queue. Folder skills are added to Queue skills and do not override them.

- **Mailbox** — select the mailbox to assign to this folder.

- **Maximum email body size** — for text mode only, the maximum email body size in characters to expose to scripts. The default is 8192 characters.

  > **Note**
  >
  > To disable body fetching for both HTML and text, set to 0.

- **Email body script format** — select the format for the email body exposed to the call arrival and other scripts. The default is HTML.

  > **Note**
  >
  > - We recommend that you use text mode and control the email body size.
  > - In HTML mode, the entire body is available/exposed in scripts, which may have an impact on network bandwidth between MS and MCS, MS performance, and MCS memory growth.
  > - In HTML mode, some types of embedded image links may be broken.

3. Click **OK**.

Edit a folder

1. On the **Folders** page, click the item to edit. The **Folder: [Name]** dialog appears.
2. Edit the information. For details, see Add a folder.
3. Click **OK**.

Delete a folder

> **Note**
>
> - CCaaS does not delete email folders that contain items. If you try to delete an email folder that contains items or a timeout occurs, a message that the operation failed appears.
> - If the system administrator has not assigned your contact center to a Messaging Server, you cannot delete an email folder.

1. On the **Folders** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion. If a warning appears that lists the folders that were not deleted, click **OK**.

Manage groups

View the Groups list

Add a group

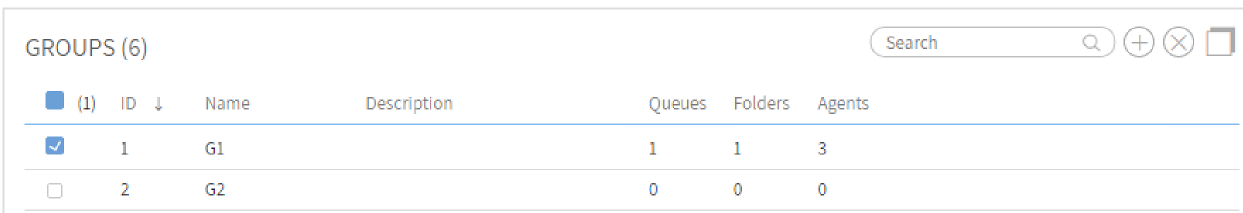
Clone a group

Edit a group

Delete a group

View the Groups list

1. On the navigation pane, click **Organization.**
2. Click the **Groups** tab. The **Groups** list appears. For navigation information, see List view and How to search.
   The Queues, Folders, and Agents columns show the number of items assigned to the group.



GROUPS (6)

(1)	ID ↓	Name	Description	Queues	Folders	Agents
☑	1	G1		1	1	3
☐	2	G2		0	0	0

Add a group

1. On the **Groups** page, click **Add**. The **New Group** dialog appears.
2. Enter the following information:
   - **Name** (required) — the name of the group.
   - **Description** — a description of the group.
   - **Block international calls** — whether to block outgoing international calls.
   - **Block long distance calls** — whether to block outgoing long distance calls.
   - **Block local calls** — whether to block outgoing local calls.
   - **Agents** — click **Add items** and select the agents for this group. See Filter for agents.
   - **Primary queues** — select the primary queues for this group.
   - **Secondary queues** — select the secondary queue for this group.
   - **Block codes** — select the block codes for this group.

     Note

     Block codes only affect long distance calls. The **Block long distance calls** check box supersedes any block codes you enter in **Block codes.**

- **Folders** — select the folders for this group.
- **Release codes** — select the release codes for this group. You can add the same release codes to multiple groups.
- **No release codes** — whether you do not want this group to use release codes.

> **Note**
> If you select **No release codes**, agents in this group can still become Available or Unavailable.

3. Click **OK**.

Clone a group

1. On the **Groups** page, select the item/s to clone.
2. Click and then click **Clone Groups**. The **Clone Groups** dialog appears.
3. Optionally added a prefix and/or suffix for the cloned groups.
4. Click **OK**.

Edit a group

1. On the **Groups** page, click the item to edit. The **Group: [Name]** dialog appears.
2. Edit the information. For details, see Add a group.
3. Click **OK**.

Delete a group

1. On the **Groups** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage interaction profiles

View the Interaction Profiles list

Add an interaction profile

Edit an interaction profile

Delete an interaction profile

Interaction profiles define the rules for how the CMS allocates calls to individual agents. They define the media types a specific agent can handle, the number of concurrent calls of each type, and any blocking or interruption rules.

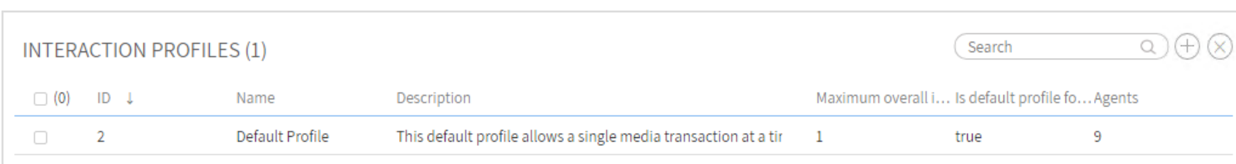
Each interaction profile contains a collection of interaction profile rules, one for each media type, although not every media type needs to be included. Each existing and new agent (personnel) is assigned to a single interaction profile. Any new agents are assigned to the profile designated as the default profile for new agents. The maximum total concurrent interactions per agent are limited to 9. If voice calls are configured to override this maximum, the limit is 10.

Multi-interaction enables an agent to simultaneously handle multiple calls, up to a configured number between one and nine. If voice calls are configured to override this maximum, the limit is 10.

In CCaaS Admin, you configure the number of interactions each agent can handle using multi-interaction profiles. You then enable multi-interaction for an agent by assigning the relevant interaction profile to the agent in the Interaction profile property on the Properties tab of the [Agent name] page. See Manage personnel properties. Alternatively, you can assign the agent as a member of a multi-interaction profile.

View the Interaction Profiles list

1. On the navigation pane, click **Miscellaneous.**
2. Click the **Interaction Profiles** tab. The **Interaction Profiles** list appears. For navigation information, see List view and How to search. For column descriptions, see Add an interaction profile. The Agents column shows the number of agents assigned to the interaction profile.



Add an interaction profile

1. On the **Interaction Profiles** page, click **Add**. The **New Interaction Profile** dialog appears.
2. Enter the following information:

- **Name** (required) — the name of the interaction profile.
- **Description** — a description of the interaction profile.
- **Is default profile for new agents** —whether you want all new agents to be assigned to this profile.

  > **Note**
  >
  > There can be only one default interaction profile. When you select the **Is default profile for new agents** check box, CCaaS automatically clears the corresponding check box on the previous default profile.

- **Maximum overall interactions** — a number between 0 and 9. A value of 0 means that agents assigned to this interaction profile cannot handle any ACD media.
- **Agents** — click **Add items** and select the agents to assign this interaction profile to. See Filter for agents.

3. Under **Internet, Phone, Email, Callback,** and **Voicemail** enter the following information:

   - **[Media type] rule maximum interactions** — a number between 0 and 9. A value of 0 means that agents assigned to this profile cannot handle this media type.
   - **[Media type] rule call weighting** — a number between 0 and 100, representing the relative weight of this media type. A value of 100 means the highest weighting. The CMS uses this value to determine which agent has the least load and should therefore take the next call.

     > **Note**
     >
     > If the weight of a media type is set to zero, the agent is reported as available during the time of a call from that media. Consequently, in reports an agent can appear as 99% available and at the same time have handled many calls.

   - **[Media type] rule media allowed** — agents assigned this interaction profile can handle calls of this media type. If you want agents assigned this interaction profile not to be allowed to handle this media type, clear the check box. Selected by default.
   - **[Media type] rule overrides maximum interactions** — agents can handle chat and email even if that agent is already handling the maximum overall interactions specified above. Not selected by default.
   - **[Media type] rule blocks other media types** — agents that are currently interacting with internet media types, can be routed only the same type of media call. When all internet media type calls are completed, the agent receives calls of another media type. Selected by default.

4. Click **OK**.

Edit an interaction profile

1. On the **Interaction Profiles** page, click the item to edit. The **Interaction Profile: [Name]** dialog appears.
2. Edit the information. For details, see Add an interaction profile.
3. Click **OK**.

Delete an interaction profile

Before you can delete an interaction profile, you must unassign the agents from it. If it is the default profile, you must also first set another interaction profile as the default.

When you delete an interaction profile, CCaaS also deletes its interaction profile rules.

1. On the **Interaction Profiles** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage legacy licenses

View the legacy Licenses list

View contact center licenses

Allocate legacy licenses to users

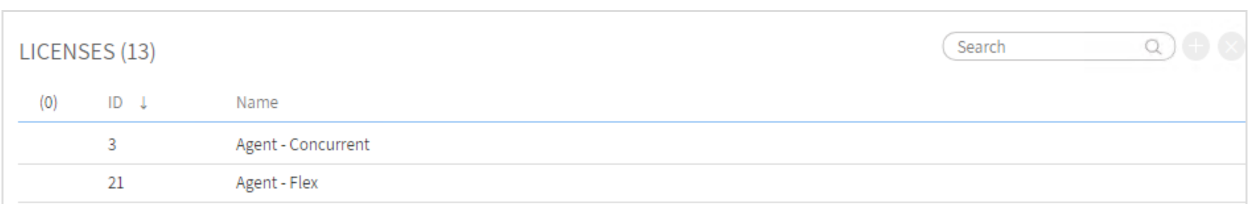
Legacy licenses are used to determine how many agents can log on per tenant. The tenant administrator can view the number of available agent licenses added to their contact center by the system administrator.

If the enforcement type is Block, the tenant's logged on agents cannot exceed the number of available licenses.

> **Note**
> Your agents may be prevented from logging on, even when they are within your available licenses limit, if some tenants do not have the Block enforcement type and exceed the number of licenses allocated to them.

View the legacy Licenses list

1. On the navigation pane, click  **Miscellaneous.**
2. Click the **Licenses** tab. The **Licenses** list appears. For navigation information, see List view and How to search.



View contact center licenses

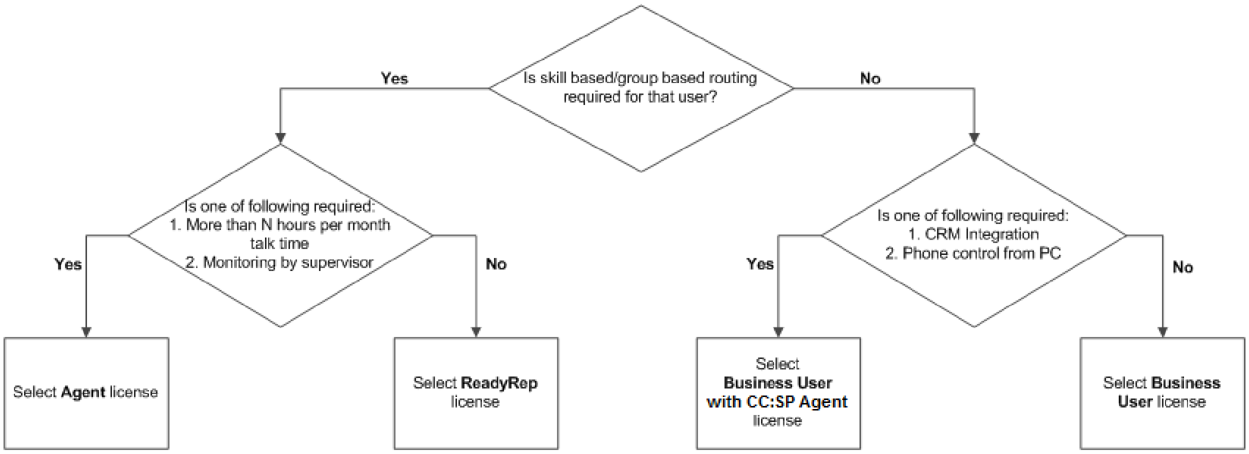
You can view the agent licenses added to your contact center.

1. On the **Licenses** page, click the **Agent - Concurrent** license. The **License: [Name]** dialog appears.
2. View the following information:
   - **Name** — the license name.
   - **Available** — the number of agent licenses allocated to your contact center.
   - **Enforcement type** — the options are:
     - **None** (default) — allow agent logons above this limit.
     - **Block** — do not allow agent logons above this limit.

3. Click **OK**.

Allocate legacy licenses to agents

For each agent, select the appropriate license, using the following flow chart as your guide. See Manage personnel parameters.



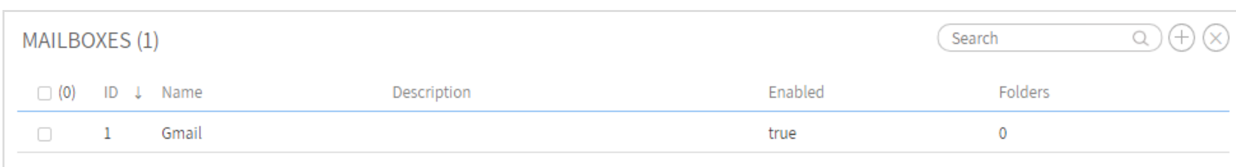
Manage mailboxes

The CCaaS messaging subsystem can interact with an external mailbox to receive and send emails. In this context, *external* means that mailbox is stored on a mail server that is external to CCaaS.

The external mailbox must be created or purchased separately and must support the IMAP, SMTP network protocols. When the mailbox exists on a mail server, you can define it in the CCaaS Admin so it can be accessed by CCaaS services. The external mailbox must have an email address. There are mail server vendors that allow adding email address aliases to a given mailbox. In this context, an alias is just another email address given to a mailbox. You can have one or more mailboxes defined.

View the Mailboxes list

1. On the navigation pane, click **Routing**.
2. Click the **Mailboxes** tab. The **Mailboxes** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a mailbox. The Folders column shows the number of folders assigned to the mailbox.



Add a mailbox

1. On the **Mailboxes** page, click **Add**. The **New Mailbox** dialog appears.
2. Enter the following information:
   - **Name** (required) — the name for CCaaS to use to identify the mailbox.
   - **Description** — a description of the mailbox.
   - **Folders** — select the folders that are associated with this mailbox.

     Note

     - If more than one folder is associated with this mailbox entity, you must define an email address alias on the mail server for this mailbox.

> - The MS performs mailbox-folder matching based on the recipient email address and the target folder email address. If an item contains more than one recipient that matches, the item is cloned to each matched folder.

- **Enabled** — whether to allow the MS to access this mailbox.

> **Note**
>
> Before enabling the mailbox, confirm that the landlord system administrator has completed the prerequisite mailbox configuration.

- **IMAP address** (required) — the address of the mail server IMAP listener.
- **IMAP port** (required) — the port on which the mail server is listening to the IMAP protocol. The default is 993.
- **SMTP address** — the address of the mail server SMTP listener.
- **SMTP port** — the port on which the mail server is listening to the SMTP protocol. The default is 587.
- **Username** — the user name to authenticate to the mail server. This name must be unique across all the service provider's tenants.
- **Password** — the password for user authentication. The value specified in this field is encrypted by the value of the Tenant Encryption Key parameter specified in Tenant Parameters by the landlord System Administrator.

> **Note**
>
> If the Tenant Encryption Key does not exist, the password cannot be saved or edited.

- **Auto connect retries** — the number of attempts to connect to the mail server before failing. The default is 3.
- **Max idle time (sec)** — the maximum time to hold idle connections before closing them (not currently in use). The default is 360.
- **Max email size in bytes** — the maximum size of an email that will be downloaded from the mailbox. Emails exceeding this limit are handled according to the policy defined in the Post MSR invalid method parameter. The default is 6000000 (bytes).
- **Max email LW size in bytes** — the maximum size of a lightweight email. Emails up to this size are downloaded in parallel with emails of size above this parameter. The default is 10000(bytes).
- **Max number of items to collect** — the maximum number of emails to download from the mailbox in each iteration. The default is 50.
- **Post MSR persisted method** (required) — select what to do with the email item stored in the mailbox inbox after it was downloaded and inserted into the Tenant Messaging Database. Possible values are:
  - **Move to processed mailbox folder** (default) — move the email item to a special folder on the mailbox (the Processed folder).
  - **Delete item** — delete the email item from the mailbox inbox.
- **Post MSR invalid method** (required) — select what to do with the email item stored in the mailbox inbox after it was downloaded but was not inserted into the Tenant Messaging Database because it was detected as invalid. Possible values are:

        - **Move to invalid mailbox folder** (default) — move the email item to a special folder on the mailbox (the Invalid folder).
        - **Delete item** — delete the email item from the mailbox inbox.
    - **Persisted emails folder name** — the name of the folder on the mailbox that CCaaS will create and use to store email items that were downloaded and stored in the Tenant Messaging Database. The default is PersistedCCSPItems.
    - **Invalid emails folder name** — the name of the folder on the mailbox that CCaaS will create and use to store email items that were downloaded but were detected as invalid and were not stored in Tenant Messaging Database. The default is InvalidCCSPItems.
    - **Deleted emails folder name** — the name of the folder on the mailbox that CCaaS will create and use during deletion of email stored in the inbox. The default is DeletedCCSPItems.
    - **IMAP secure connection type** (required) — select the type of the secured connection to the mail server when using the IMAP protocol. The options are:
        - **Auto** (default) — auto decide whether to use SSL or TLS.
        - **SslOnConnect** — the connection should immediately use SSL or TLS encryption.
        - **StartTls** — elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server.
    - **SMTP secure connection type** (required) — select the type of the secured connection to the mail server when using the SMTP protocol. The options are:
        - **Auto** (default) — auto decide whether to use SSL or TLS.
        - **SslOnConnect**— the connection should immediately use SSL or TLS encryption.
        - **StartTls** — elevates the connection to use TLS encryption immediately after reading the greeting and capabilities of the server.

3. Click **OK**.

Edit a mailbox

1. On the **Mailboxes** page, click the item to edit. The **Mailbox: [Name]** dialog appears.
2. Edit the information. For details, see Add a mailbox.
3. Click **OK**.

Delete a mailbox

1. On the **Mailboxes** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage permission profiles

> **Note**
> CCaaS UI was previously called TouchPoint.

Default permission profiles

View the Permission Profiles list

Add a permission profile

Edit a permission profile

Delete a permission profile

Permissions are assigned to users through permission profiles that are designed so that a number of users can be assigned a set of permissions simultaneously and uniformly.

> **Note**
> - Only users with the default Administrator permission profile can manage permission profiles.
> - By default, the Supervisor profile has supervisory privileges over the whole contact center. To limit a supervisor's privileges to particular groups, create a group supervisor. See Add a permission profile.

Permission profiles control access to the following objects, so it is best to configure these objects before creating the permission profiles:

- Groups
- Queues
- Teams

Default permission profiles

The predefined permission profiles are:

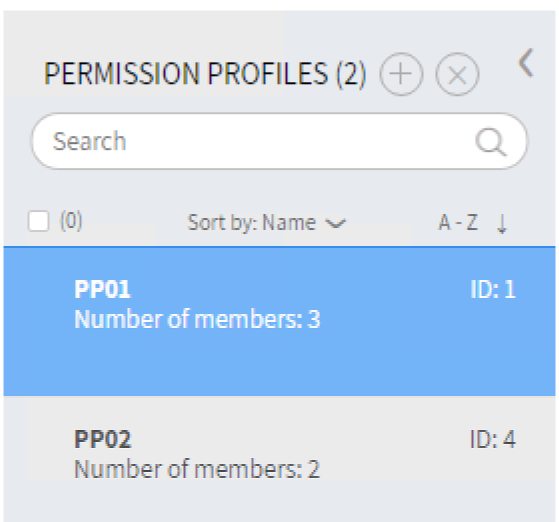
- **Administrator and Agent**
  - Can set up and configure anything in the tenant contact center, including new permission profiles.
  - Can use CCaaS UI.
  - Cannot view CCaaS reports or play back recordings.
- **Administrator and Supervisor**
  - Can set up and configure anything in the tenant contact center, including new permission profiles.
  - Can view CCaaS Historical Reports and Dashboard reports for the whole tenant.
- **Administrator**
  - Can set up and configure anything in the tenant contact center, including new permission profiles.
  - Cannot view CCaaS reports or play back recordings.
  - Cannot use CCaaS UI.

- **Agent**
  - Can use CCaaS UI.
  - Cannot view CCaaS reports or play back recordings.
  - Cannot set up and configure anything in the tenant contact center.
- **Supervisor (tenant-wide supervisor)**
  - Can view CCaaS Historical Reports and Dashboard reports for the whole tenant.
  - Can play back recordings for the whole tenant.
  - Cannot set up and configure anything in the tenant contact center.
- **Team Supervisor**
  - Can supervise the teams to which they are assigned. Can also view reports and play back recordings only for the teams to which they are assigned.
  - Can use CCaaS UI.
  - Cannot set up and configure anything in the tenant contact center.

> **Note**
> Users not assigned a permission profile have the permissions of agents.

View the Permission Profiles list

1. On the navigation pane, click **Organization.**
2. Click the **Permission Profiles** tab. The **Permission Profiles** list appears. For navigation information, see Card view and How to search.



Add a permission profile

1. On the **Permission Profiles** page, click **Add**. The **New permission profile** page appears.
2. Click the **Properties** tab and enter the following information:
   - **Name** (required) — the name of the profile.
   - **Description** — a description of the profile.
   - **Allow create/delete** — whether to allow an administrator with restricted permissions to create new objects or delete existing objects. If not selected, the administrator can only modify the properties of existing objects.
   - **Members** — click **Add items** and select the agents to assign the permission profile to. See Filter for agents.
3. Click the **Permissions** tab and assign the permission to the objects, as required.
4. Click the **Groups** tab and assign the Report, Administer, Playback, and/or Supervise permissions to the groups, as required.
5. Click the **Queues** tab and assign the Report and Administer permissions to the queues, as required.
6. Click the **Teams** tab and assign the Report, Administer, Playback, and/or Supervise permissions to the teams, as required.
7. Click **Save changes**.

Edit a permission profile

1. On the **Permission Profiles** page, click the card of the item to edit. The **[Permission profile name]** page appears.
2. Edit the information. For details, see Add a permission profile.
3. Click **OK**.

Delete a permission profile

1. On the **Permission Profiles** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage personnel

> **Note**
> CCaaS UI was previously called TouchPoint.

View the Agents list

Add an agent

Add a phone agent

Clone an agent

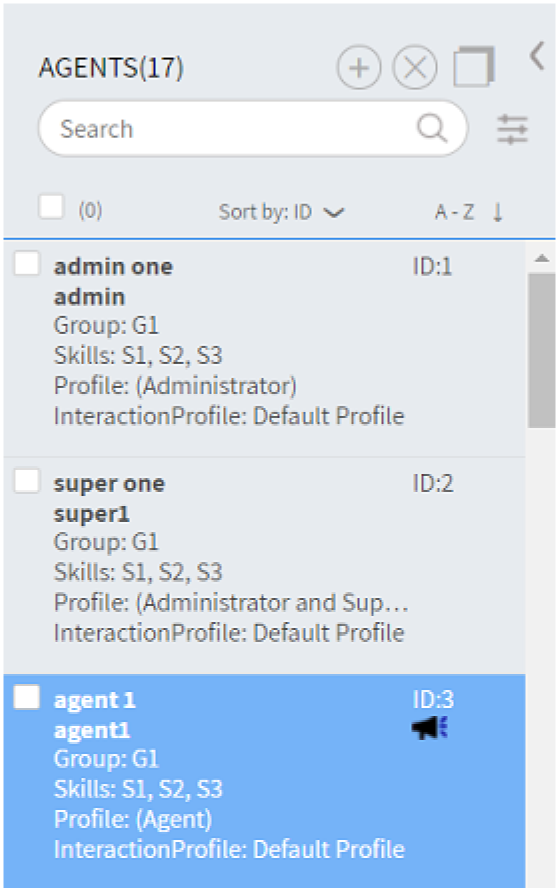
Edit an agent

Delete an agent

View the Agents list

1. On the navigation pane, click  **Organization.**
2. If necessary, click the **Personnel** tab. The **Agents** list appears. For navigation information, see Card view, How to search, and How to filter.

   The  icon indicates that the agent is campaignable.



Add an agent

> **Note**
>
> - If you are adding a phone agent, see Add a phone agent before proceeding.
> - If you are adding a supervisor or administrator, add in the same way as an agent but select the appropriate Profile on the Properties tab. See Default permission profiles.

1. On the **Agents** page, click **Add**. The **New Agent** page appears.
2. Enter the following information, arranged on the following tabs:
   - Properties
   - Phone settings
   - Parameters
3. Click **Save changes**.

Add a phone agent

In some instances, agents may be constrained to the use of only a circuit switched phone or IP phone. This may be due to how your contact center is configured, or if the agent is traveling without a computer and still needs to service calls, or perhaps in the event of a disaster.

Since the agent is operating without a computer, many of the functions that are available through CCaaS UI are not available for the Phone Agent.

Phone agents are created in exactly the same manner as other agents. You must:

- Assign the agent a *numeric* Login ID and *numeric* Password.
- Enter the agent's phone number into the **Phone ANI** field of the personnel record.
- Configure the area code and country.

> **Note**
>
> - Phone agents can use the same numeric Login ID and Password to log on normally from a computer.
> - Phone agents can only be created on the internal VCS stack.

Clone an agent

1. On the **Agents** page, select the item/s to clone.
2. Click and then click **Clone Agents**. The **Clone Agents** dialog appears.
3. Optionally added a prefix and/or suffix for the cloned agents.
4. Click **Set Password**. The **Change password** dialog appears.
5. Type a new password that meets your AD policy, type the password again to confirm it, and then click **OK**.
6. Click **OK**.

Edit an agent

1. On the **Agents** page, click the card of the item to edit. The **[Agent name]** page appears.
2. Edit the information. For details, see Add an agent.
3. Click **OK**.

Delete an agent

1. On the **Agents** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage personnel properties

> **Note**
>
> - Tenant administrators, with Administrator, Administrator Admin and Administrator Supervisor roles, now need explicit permission to access each admin application (specified in **Allowed Admin applications**).
> - The landlord or reseller administrator specifies whether the tenant administrator can change the allowed admin applications for themselves and other users. (**Can edit Allowed Admin applications**).
> - Tenant administrators with more than one allowed admin application, can log in using Unified Admin.

On the **New Agent/[Agent name]** page, on the **Properties** tab, enter the following information:

- **Login ID** (required) — a unique name for the agent. This name must not contain spaces, underscores, or special characters.
- **Change password** — click and in the **Change password** dialog, type a password that meets your AD policy.
- **First name** (required) — the agent's first name.
- **Last name** (required) — the agent's last name.
- **Description** — a description of the agent.
- **Profile** — select from the list of available permission profiles. Default profiles are enclosed in parentheses and cannot be changed. Leave blank to assign the default agent profile. See Manage permission profiles.

  > **Note**
  >
  > - The list of available permission profiles to assign to the agent is limited to the permission profiles that contain only the groups that are included in your own profile.
  > - If you change an agent's permission profile, to avoid potential inconsistent behavior or errors inside CCaaS UI for operations regulated by different permission profiles, that agent must log off from CCaaS UI and log on again.

- **Skills** — select this agent's skills from the list of available skills that you added. See Manage skills.
- **Set skills weight** — click and then in the **Set Skills Weight** dialog, select the weight for the skills that have weighting enabled: 0 is high and 100 is low.

  > **Note**
  > Skill weighting must first be enabled by the landlord in tenant properties and then enabled for the individual skill. See Manage skills.

- **Groups** — select from the list of available groups that you created. See Manage groups.
- **Block codes** — select from the list of available codes that you created for blocking international, long distance, and local calls. See Manage block codes.
- **Interaction profiles** — select from the list of available interaction profiles, which determine the maximum number and types of calls that this agent can handle. See Manage interaction profiles.

  > **Note**

> If you change an agent's interaction profile, the agent's load level displayed in Dashboard changes only when the agent finishes the current call or a new call is added to the agent.

- **Teams** — select from the list of available teams that you created. See Manage teams.
- **Time zones** — select from the list of available time zones that you created. See Manage time zones.
- **Can edit Allowed Admin applications** — whether to allow the admin user to change the allocated Admin applications for themselves and other users. This property is only visible to landlord administrators and reseller administrators.
- **Allowed Admin applications** — select from the list of available admin applications. This property is disabled if the user's profile is not an administrator-type role.

> **Note**
>
> - If the user's profile is changed to an administrator-type role, this property is only enabled when the profile change is saved.
> - When a user is moved from a non-administrator role to an administrator-type role, they are assigned all the admin applications by default.

- **Is campaignable** — whether to allow the agent to participate in campaigns.
- **Can request consultation** — whether the agent can request a chat consultation during a call.

Manage personnel phone settings

> **Note**
> CCaaS UI was previously called TouchPoint.

On the **New Agent/[Agent name]** page, on the **Phone settings** tab, view/enter the following information:

- **Phone ANI** — the identifier used for call routing or billing. This is an optional field that can be required by your telephone carrier. ANI is different from Caller ID, but might be used by a telephone carrier to display caller identity to the called party. The value of this field is usually provided by the telephone company and is numeric text.
- **Caller ID** — the identity the agent presents to a called party. This value can be text or a telephone number.
- **DNIS** (read only) — the DNIS assigned to the user. The DNIS serves as the personal voicemail User ID.
- **Country code** — the agent's country code. This code can be a maximum of three numeric digits and can have a leading plus sign (+).
- **Area code** — the agent's area code. This code can be a maximum of 12 numeric digits.
- **Voice device type** — the agent's voice device. The options are:
  - **NotSet** (default) — set in CCaaS UI by the agent
  - **SIP** — CCaaS UI provides a SIP voice terminal
  - **H323** — CCaaS UI provides an H.323 voice terminal
  - **VoiceDevice** — a phone
  - **CommunicatorClient** — not in use
- **Voice device address** — the agent's phone IP or extension in E.164 or SIP URI format. For Teams, use the agent's phone number associated with it.
- **Block local calls** — whether to block outgoing local calls.
- **Block long distance calls** — whether to block outgoing long distance calls.
- **Block international calls** — whether to block outgoing international calls.
- **Auto release on call pickup** — whether to have the agent automatically enter the released state when a call is picked up. The agent needs to manually make themselves available when after-call work is complete.
- **Auto release on ring timeout** — the number of pickup failures after which the agent automatically enters the released state. The default is 0 (disabled).
- **Automatic answer** — whether to have CCaaS UI automatically answer calls when they are delivered.
- **IP phone password** — the numeric password for the IP phone directly controlled by CCaaS.
- **Voicemail** — whether to enable personal voicemail. Personal voicemail is stored physically in the recording database and is unrelated to ACD-routed voicemail.
- **Mailbox PIN** — the initial numeric password that the agent enters to access their personal voicemail box. The agent can change the PIN after logging on to the voicemail system. To log on to voicemail, agents use their direct extension as the user ID and the Mailbox PIN as a password.
- **KCO mode** — whether to enable the agent to remain connected to CCaaS through an alternative device for the duration of their shift.

- **Shared mailbox** — the agent ID of the shared mailbox.
- **Use SRTP** — whether to use SRTP on the Agent leg.

> **Note**
>
> If **Use SRTP** is select for the tenant, it is used for the agent irrespective of the above setting. See Manage tenant parameters.

Manage personnel parameters

> **Note**
>
> CCaaS UI was previously called TouchPoint.

On the **New Agent/[Agent name]** page, on the **Parameters** tab, enter the following information:

- **Login license type** — the license to assign to the agent. See Allocate legacy licenses to agents.
- **CosmoCorder license** — whether to assign this license.
- **CosmoConnector license** — whether to assign this license.
- **ScreenRecording license** — whether to assign this license.
- **External email address** — the email address for delivery of personal voicemail. Agents with personal voicemail enabled can have their personal voicemail delivered as email sound file attachments. The emails containing the attachments are sent to this external email address, which is not related to ACD-routed emails.
- **Agent can change password** — whether to allow the agent to change their CCaaS UI password. If not selected, password settings do not appear in CCaaS UI.
- **Available upon login** — whether to have the agent automatically become available when logging on to CCaaS UI.
- **CRM URL** — the URL of the tenant's CRM.
- **CRM user ID** — the agent's user ID for the tenant's CRM.
- **CRM password** — the agent's password for access to the tenant's CRM.
- **Block agent to agent calls** — whether to prevent the agent from calling another agent.
- **Block xfer/conf to agent** — whether to prevent the agent from transferring or conferencing calls to another agent.
- **Block call/xfer to system** — whether to prevent the agent from transferring calls to entry points.
- **Preferences edit by agent** — whether the agent can edit their preferences in CCaaS UI. The options are:
  - **Deny** — preferences are not displayed in CCaaS UI.
  - **Allow** (default) — the agent can permanently configure CCaaS UI preferences.
  - **Allow per session** — obsolete.
  - **Read-only** — preferences are displayed but selection is disabled in CCaaS UI.
- **Encrypted recording restrictions** — the restrictions that apply to supervisors when playing back encrypted recordings. The default is None.

  > **Note**
  >
  > Encrypted recording restrictions for the tenant are set in the **Tenant Properties** dialog, on the **Parameters** tab (see Manage tenant parameters). To override this setting for the agent, select a value other than None.

Manage phone aliases

Phone aliases can be used to create easily memorized nicknames for particular phone numbers, or to map to particular numbers or individuals within your organization. They can be thought of as extensions, but they can be any set of alphanumeric characters, including words or short phrases. When assigning words or phrases to an alias, any users who would be likely to use the alias should be made aware of its existence.

Use wildcards in phone aliases

A common use for this feature is to create shortcut dialing numbers, similar to speed dialing numbers, for a company with offices in different locations. If, for example, all of the extensions in your local office begin with the digit 4 and the extensions in another office begin with 7, you can assign the alias 7000 to the number +1516557000. Then a person in your office only has to dial 7000 to connect to the person with that number in the other office.

You can also use a question mark as a wildcard to replace any digits in both the alias and the number to be dialed. To extend the above example further, you could assign the alias 7??? to the phone number +1516557??? to create shortcuts to all of the extensions in that other office. In a similar manner, you could assign the alias 4??? to your +1631940??? main office phone number.

View the Phone Aliases list

1. On the navigation pane, click **Miscellaneous.**
2. Click the **Phone Aliases** tab. The **Phone Aliases** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a phone alias.

(0)	ID	Phone aliases	International number
	1	UK	+44
	2	USA	+1

Add a phone alias

1. On the **Phone Aliases** page, click ⊕ **Add**. The **New phone alias** dialog appears.
2. Enter the following information:
    - **Phone alias** (required) — the name, number, or other significant identifier.
    - **International number** (required) — the **+** (international standard format) phone number that is dialed when the alias is used. This number must follow the international standard format, but does not necessarily have to be in another country.
3. Click **OK**.

Edit a phone alias

1. On the **Phone Aliases** page, click the item to edit. The **Phone alias: [Name]** dialog appears.
2. Edit the information. For details, see Add a phone alias.
3. Click **OK**.

Delete a phone alias

1. On the **Phone Aliases** page, select the item/s to delete.
2. Click ⊗ **Delete** and then confirm the deletion.

Manage queues

View the Queues list

Add a queue

Clone a queue

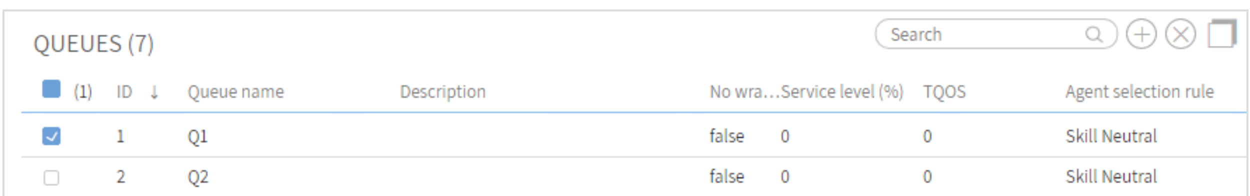
Edit a queue

Delete a queue

> **Caution**
> The information entered in the **Queue: [Name]** dialog dictates call flow, sets priorities, and triggers events effecting calls arriving at your contact center. It determines the quality of service your business strives to provide its customers. Therefore, this information must be agreed to or provided by your contact center's affected business units.

View the Queues list

1. On the navigation pane, click **Routing**.
2. Click the **Queues** tab. The **Queues** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a queue.



Add a queue

1. On the **Queues** page, click **Add**. The **New Queue** dialog appears.
2. Enter the following information:

   - **Queue name** (required) — the name of the queue. Queue names can be a maximum of 32 characters.
   - **Description** — a description of the queue.
   - **Primary in groups** — select the primary group or groups for this queue.
   - **Secondary in groups** — select the secondary group or groups for this queue.
   - **Skills** — select the skill requirements to assign to calls that arrive at this queue without a skill assigned in the IVR script.
   - **Wrap-up codes** — if required, select the codes.
   - **No wrap-up** — whether the queue does not require wrap-up codes.

- **Timeout in queue** — the maximum amount of time a caller should wait in a queue before the call times out. When a caller's wait in queue exceeds this time, the In Queue Timeout script specified with Designer runs. When a queue is created, its default in queue timeout is 5 minutes (300 seconds).

  > **Note**
  > Create a separate queue for email (MCS) messages.

  For a contact center that receives many email messages, the in queue timeout should be as large as possible. When the in queue timeout expires, the MCS takes all calls from the Call Matcher, runs the in queue timeout script and then resubmits them back to the Call Matcher. This would consume excessive bandwidth if there are a large number of email messages.

  For example, if the contact center receives 10,000 message calls a day and it takes 2 days for all the available agents to answer all 10,000 message calls, a reasonable in queue timeout for the message queue would be 2 days (172800 seconds).

- **Timeout pickup** — the pickup timeout for the queue. When a call rings to an agent and the ringing time exceeds this time and the agent has not answered the call, the *Pick-up Timeout* script specified with Designer runs and routes the call to the next available agent.

  > **Caution**
  > By default, timeout occurs at 75% of the value that you specify. For more information, see **PickUpTimeoutMultiplyer** registration key in the *CCSP Registry Key Reference*.

  > **Note**
  > If you set the pickup timeout to 0, all calls routed to an agent on that queue (incoming or transfer to system calls) ring indefinitely on the first chosen agent from that queue.

- **Timeout wrap-up** — the amount of time allowed for wrap-up activity before the default wrap-up code is selected.
- **Service level (%)** — obsolete.
- **TQOS (sec)** — the TQoS for the queue.
- **Agent selection rule** — select the appropriate level.

3. Click **OK.**

Clone a queue

1. On the **Queues** page, select the item/s to clone.
2. Click  and then click **Clone Queues**. The **Clone Queues** dialog appears.
3. Optionally added a prefix and/or suffix for the cloned queues.
4. Click **OK**.

Edit a queue

1. On the **Queues** page, click the item to edit. The **Queue: [Name]** dialog appears.
2. Edit the information. For details, see Add a queue.
3. Click **OK**.

Delete a queue

1. On the **Queues** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage release codes

View the Release Codes list

Add a release code

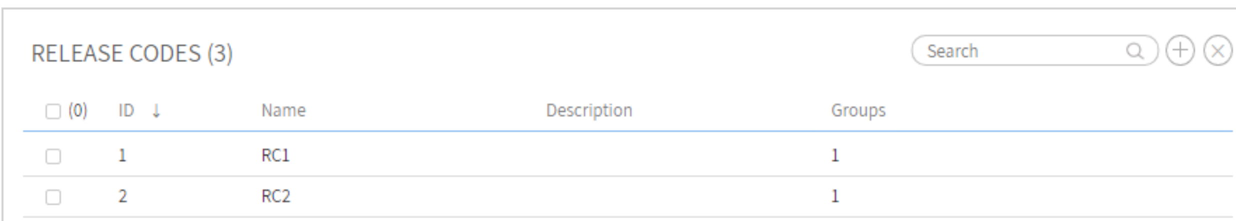
Edit a release code

Delete a release code

For information about release codes that are assigned to groups, see Add a group.

View the Release Codes list

1. On the navigation pane, click **Routing**.
2. Click the **Release Codes** tab. The **Release Codes** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a release code. The Groups column shows the number of groups assigned to the release code.



Add a release code

1. On the **Release Codes** page, click **Add**. The **New Release Code** dialog appears.
2. Enter the following information:
   - **Name** (required) — the name of the release code.
   - **Description** — a description of the release code.
3. Click **OK**.

Edit a release code

1. On the **Release Codes** page, click the item to edit. The **Release Code: [Name]** dialog appears.
2. Edit the information. For details, see Add a release code.
3. Click **OK**.

Delete a release code

1. On the **Release Codes** page, select the item/s to delete.
2. Click ⊗ **Delete** and then confirm the deletion.

Manage skills

View the Skills list

Add a skill

Clone a skill

Bulk assign agents to skills

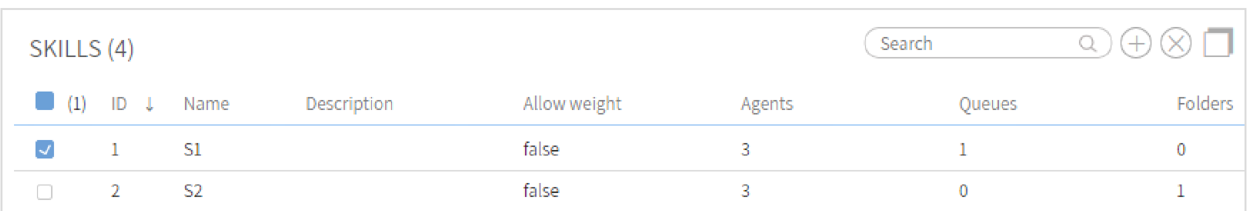
Edit a skill

Delete a skill

To assign weights to skills by agent, see Manage personnel properties.

View the Skills list

1. On the navigation pane, click **Organization.**
2. Click the **Skills** tab. The **Skills** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a skill. The Agents, Queues, and Folders columns show the number of items assigned to the skill.



Add a skill

1. On the **Skills** page, click **Add**. The **New Skill** dialog appears.
2. Enter the following information:
    - **Name** (required) — the name of the skill.
    - **Description** — a description of the skill.
    - **Allow weight** — whether to enable skill weighting for this skill.
    - **Agents** — click **Add items** and select the agents that have this skill. See Filter for agents.
    - **Queues** — select the groups that require this skill.
    - **Folders** — select the folders that require this skill.
3. Click **OK**.

Clone a skill

1. On the **Skills** page, select the item/s to clone.
2. Click and then click **Clone Skills**. The **Clone Skills** dialog appears.
3. Optionally added a prefix and/or suffix for the cloned skills.
4. Click **OK**.

Bulk assign agents to skills

1. On the **Skills** page, select the skills.
2. Click and then click **Assign Agents to Skills**. The **Assign Agents to Skills** dialog appears.
3. Under Agents, click **Add items**, select the agents, and click **OK**. See Filter for agents.
4. Click **OK**.

Edit a skill

1. On the **Skills** page, click the item to edit. The **Skill: [Name]** dialog appears.
2. Edit the information. For details, see Add a skill.
3. Click **OK**.

Delete a skill

1. On the **Skills** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage SSO permissions

Landlord and tenant administrators can create an SSO permission entry to control the users that can access one or more custom SSO applications. The SSO permission can be used to:

- Allow specific permission profiles to be able to access custom SSO applications.
- Override the tenant profile permissions for a custom SSO application that have been set at the landlord level.

View the SSO Permissions list

1. On the navigation pane, click **Organization.**
2. Click the **SSO Permissions** tab. The **SSO Permissions** list appears. For navigation information, see List view and How to search.

SSO PERMISSIONS (3)

(0)	ID	Name ↓	Description	All profiles allowed
	2	Admin access		false
	3	All access		true
	1	Supervisor access		false

Add an SSO permission

1. On the **SSO Permissions** page, click **Add**. The **New SSO Application Permission** dialog appears.
2. Enter the following information:
   - **Name** (required) — the name of the SSO permission.
   - **Description** — a description of the SSO permission.
   - **Custom SSO applications** — select the custom SSO applications to which this SSO permission applies.
   - **All profiles allowed** — whether all tenant defined users (administrators, supervisors, agents, permission profile users) are allowed to use the assigned custom SSO applications.

     > **Note**
     > This overrides any tenant permissions for the application that have been set at the landlord level.

- **Allowed profiles when all profiles allowed not set** — select the pre-defined tenant and custom permission profiles that are allowed to use this application. This list is only used for restricting access when **All profiles allowed** is not selected.

  > **Note**
  > This overrides any tenant permissions for the application that have been set at the landlord level.

3. Click **OK**.

Edit an SSO permission

1. On the **SSO Permissions** page, click the item to edit. The **SSO Application Permission: [Name]** dialog appears.
2. Edit the information. For details, see Add an SSO permission.
3. Click **OK**.

Delete an SSO permission

1. On the **SSO Permissions** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage teams

View the Teams list

1. On the navigation pane, click **Organization.**
2. Click the **Teams** tab. The **Teams** list appears. For navigation information, see List view and How to search.
   The Agents column shows the number of agents assigned to the team.

Add a team

1. On the **Teams** page, click **Add**. The **New Team** dialog appears.
2. Enter the following information:
   - **Name** (required) — the name of the team.
   - **Description** — a description of the team.
   - **Agents** — click **Add items** and select the agents in the team. See Filter for agents.
3. Click **OK**.

Bulk assign agents to teams

1. On the **Teams** page, select the teams.
2. Click and then click **Assign Agents to Teams**. The **Assign Agents to Teams** dialog appears.
3. Under Agents, click **Add items**, select the agents, and click **OK**. See Filter for agents.
4. Click **OK**.

Edit a team

1. On the **Teams** page, click the item to edit. The **Team: [Name]** dialog appears.
2. Edit the information. For details, see Add a team.
3. Click **OK**.

Delete a team

1. On the **Teams** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage time zones

View the Time Zones list

Add a time zone

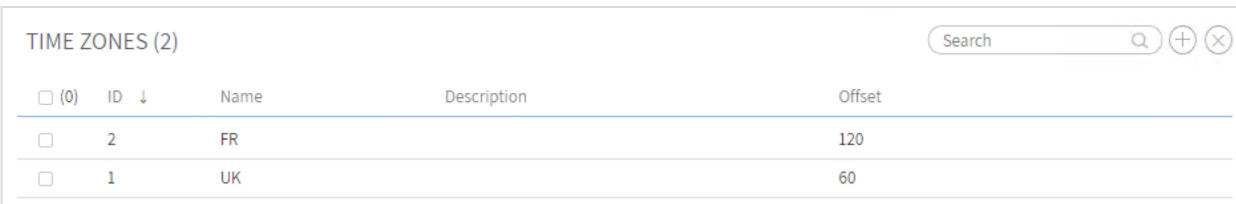
Edit a time zone

Delete a time zone

For information about setting the default time zone, see Manage other tenant properties.

View the Time Zones list

1. On the navigation pane, click **Miscellaneous.**
2. Click the **Time Zones** tab. The **Time Zones** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a time zone.


TIME ZONES (2)

(0)	ID ↓	Name	Description	Offset
	2	FR		120
	1	UK		60

Add a time zone

1. On the **Time Zones** page, click **Add**. The **New Time Zone** dialog appears.
2. Enter the following information:
   - **Name** (required) — the name of the time zone.
   - **Description** — a description of the time zone.
   - **Offset** (required) — the offset from Greenwich Mean Time (GMT) in minutes.
3. Click **OK**.

Edit a time zone

1. On the **Time Zones** page, click the item to edit. The **Time Zones: [Name]** dialog appears.
2. Edit the information. For details, see Add a time zone.
3. Click **OK**.

Delete a time zone

1. On the **Time Zones** page, select the item/s to delete.
2. Click **Delete** and then confirm the deletion.

Manage wrap-up codes

View the Wrap-Up Codes list

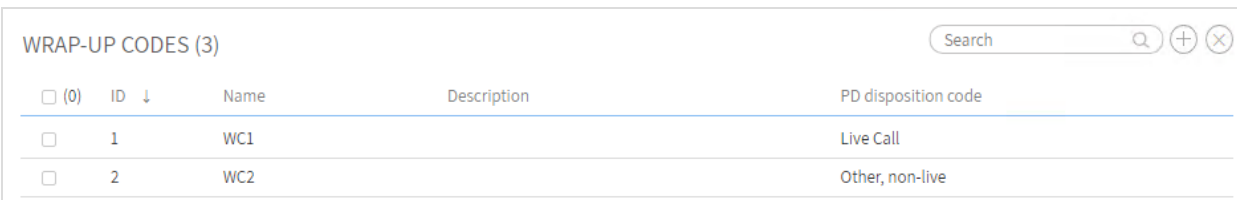
Add a wrap-up code

Edit a wrap-up code

Delete a wrap-up code

View the Wrap-Up Codes list

1. On the navigation pane, click **Miscellaneous.**
2. Click the **Wrap-Up Codes** tab. The **Wrap-Up Codes** list appears. For navigation information, see List view and How to search. For column descriptions, see Add a wrap-up code.



Add a wrap-up code

1. On the **Wrap-Up Codes** page, click **Add**. The **New Wrap-Up Code** dialog appears.
2. Enter the following information:
   - **Name** (required) —the name of the wrap-up code.
   - **Description** — a description of the wrap-up code.
   - **PD disposition code** — not enabled.
3. Click **OK.**

Edit a wrap-up code

1. On the **Wrap-Up Codes** page, click the item to edit. The **Wrap-Up Code: [Name]** dialog appears.
2. Edit the information. For details, see Add a wrap-up code.
3. Click **OK**.

Delete a wrap-up code

1. On the **Wrap-Up Codes** page, select the item/s to delete.
2. Click ⊗ **Delete** and then confirm the deletion.