# Agent Administration



# Agent Administration Tasks

## Create Voice-Only Agent

### Before you begin

You must ensure that you have already set up agent desk settings before configuring agents.

### Procedure

**Step 1** Create an Agent record by selecting **ICM Configuration Manager** > **Tools** > **Explorer Tools** > **Agent Explorer**.

If you want to associate this agent with an existing Person record, select the **Select Person** button.

**Important** Do not change an agent's ID while the agent is logged in to the agent desktop.

**Note** This step creates an Agent record associated with the Person record.

- Agent IDs can be up to nine digits long. If you are using Agent ID in the ICM Dialed Number Plan, ensure that you do not configure Agent ID to be the same as an Agent extension number on Unified CM. In this scenario, if the agent makes the call from the Agent Desktop, the call cannot be routed through an ICM script.
- If you change the Agent ID (Peripheral ID), you must cycle the PG to populate the new agent ID and information in the supervisor desktop.

**Step 2** Enter the agent information and click **Save**.

This step creates the Agent record.

If you did not use the **Select Person** button to associate the agent with an existing Person record, a new Person record is automatically created for the agent.

**Note** You can also add many agents at one time using the Bulk Configuration tool.

**Caution** Adding an agent is no longer allowed, in the following conditions:

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

# Delete Voice-Only Agent

You logically delete agents using the Agent Explorer tool. You cannot delete agents from the Agent Explorer until you remove them from any teams using the Agent Team List tool. If agents exist in script references, use the Script Reference tool to find any existing references, then use the Script Editor application to delete that script. Agents still exist in the deleted objects databases until permanently deleted.

**Note**

- For scripting and reporting purposes, if you configure the script to send a call directly to an agent and that agent is permanently deleted, the call/script fails. Also, you cannot run historical reports for permanently deleted agents.
- If you delete all the agents from a team, that team will not be available in Cisco Finesse.

### Procedure

**Step 1** Select **ICM Configuration Manager** > **Tools** > **Explorer Tools** > **Agent Explorer**.

**Note** If this was the last or only Agent record associated with the Person record for this agent, then the associated Person record is also deleted.

**Step 2** Highlight the agent and select **Delete**.

Deletes the agent as well as the associated person.

**Step 3** Select **ICM Configuration Manager** > **Tools** > **Miscellaneous Tools** > **Deleted Objects**.

**Step 4** Highlight the Agent table name in the **Tables with Deleted Records** window, then highlight the agent in the Deleted Records of the "Agent" Table window and select **Delete**.
The agent is permanently deleted from the database.

# Designate Agent Supervisor

You can identify an agent as a supervisor.

If you define an agent as a supervisor:

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

To create an agent who is a supervisor:

**Procedure**

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

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

**Step 3** Click **Add Agent**.

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

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

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

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

# Delete Agent Supervisor

When you create a new agent, you can also identify the agent as a supervisor. You can remove an agent's designation as a supervisor.

The steps to delete an agent supervisor are as follows:

### Procedure

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

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

**Step 3** Select the agent whose supervisor designation you want to remove.

**Step 4** Open the **Agent** tab.

**Step 5** Uncheck the **Supervisor** check box.

**Step 6** When finished, click **Save**.

# Create Agent Team

After adding agents with the Agent Explorer tool, you can create agent teams with the Agent Team List tool.

### Procedure

**Step 1** Access the Agent Team List tool by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Team List**.

**Step 2** Select **Retrieve**, and then select **Add** to add a new agent team.

Allows you to begin defining a new agent team. Complete the window, adding desired agents to the team.

**Step 3** Select the **Members** tab.

Allows you to select agents to add to the team.

**Step 4** Select the **Supervisor** tab.

Allows you to designate a supervisor for the team.

With Unified CCE, assign both a primary and a secondary supervisor to each agent team.

# Delete Agent Team

You delete agent teams with the Agent Teams List tool.

### Procedure

**Step 1** Access the Agent Team List tool in the Configuration Manager by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Team List**.

**Step 2** Select **Retrieve** to obtain the current list of teams.

**Step 3** Highlight the team you want to delete and select **Delete**.

**Step 4** Select **Save** to save your changes.

# Configure Not Ready Reason Codes

**Procedure**

**Step 1** Select **ICM Configuration Manager** > **Tools** > **List Tools** > **Reason Code List**.

**Example:**

**Note** If you are using the agent desktop, make sure the Reason Codes match the codes on the desktop. Unified ICM Reason Codes appear in the Agent Not Ready reports, but the agent actually selects the desktop code, so these codes must match to avoid confusion. Configure predefined Not Ready Reason Codes so their text appears in the reports.

**Step 2** Enable the Agent event detail option by selecting **ICM Configuration Manager** > **Tools** > **Explorer Tools** > **PG Explorer**, and then selecting the Unified CM peripheral.

**Step 3** Select the Agent event detail check box on the **Agent Distribution** tab to enable reporting on Not Ready Reason Codes.

**Step 4** Configure the Not Ready Reason Codes on the desktop.

# Agent Feature Configuration

This section describes how to perform the following tasks:

- Configure Unified CCE for Redirection on No Answer situations on IP IVR and Unified CVP
- Configure automatic wrap-up
- Configure supervisor assist and emergency alert situations

## Configure Unified CCE for Redirection on No Answer on IP IVR

**Important** Unified CM is the Unified ICM Routing Client that ensures the call arrives at the right destination.

**Procedure**

**Step 1** Configure agent desk settings by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Desk Settings List**.

Allows you to define the following:

- A Redirection on No Answer time
- Redirection on No Answer dialed number (to access the Redirection on No Answer script defined in Step 3, below)

**Note** The Redirection on No Answer timer is not applicable if the **Auto answer** option is enabled because the Redirection on No Answer feature and Force Answer are mutually exclusive. If both are defined, Auto answer takes precedence over Redirection on No Answer.

**Step 2** Set up the call type by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Call Type List**.

This step sets up the call type and associates it with the dialed number and the routing script.

**Step 3** Using the Script Editor, create a routing script to handle Redirection on No Answer situations.

This step allows you to define routing logic used for situations when an assigned agent does not answer.

**Important** This script queues the call at the highest priority in the skill group(s) defined within the call variables; otherwise, the call is no longer the first call to be routed off of the queue, as it was when it was first assigned to the (unavailable) agent. Also, call variables that were set in the original routing script are still present in the ring-no-answer script. Consequently, you might want to set variable values in one script that can be checked and acted upon in the other script.

**Note**

- If you configure the Redirection on No Answer timer in the Unified ICM agent desk settings, it is not necessary to configure the Unified CM Call Forward No Answer fields for the agent extensions in the Unified CM configuration. If you want to configure them for cases when an agent is not logged in, set the Unified CM system service parameter for the Unified CM Call Forward No Answer timer at least 3 seconds higher than the Unified ICM Redirection on No Answer timer on each of the Unified CM nodes.
- If you want to ensure that Redirection on No Answer calls adversely affect the service level, define the service level threshold to be less than the Redirection on No Answer timer at the call type and service.

# Configure Unified CCE for Redirection on No Answer on Cisco Unified CVP

For Unified CCE systems in which Unified CVP is deployed, the Unified CM does not control Unified CVP and cannot send an unanswered call back to Unified CVP for requeuing. You configure the Re-route on Redirection on No Answer feature to only make the agent state “Not Ready” when the agent does not answer a call. Use the Unified CVP Target Requery feature to re-queue the call. For more information, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide.

**Important** Unified CM does not control the queuing platform (Unified CVP); therefore, Unified CM cannot send the call back to Unified CVP for requeuing.

### Procedure

**Step 1** Configure agent desk setting by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Desk Settings List**.

Allows you to define the following:

- A Redirection on No Answer time: Set this number less than the number set for the No Answer Timeout for the Target Requery that you set in Unified CVP (causes agent to be made unavailable after the Redirection on No Answer timer expires, but cannot invoke the Redirection on No Answer mechanism to re-route the call—see Step 3, below)
- Redirection on No Answer dialed number (to access the Redirection on No Answer script): Leave this field blank

**Note** The Redirection on No Answer timer is not applicable if Auto-answer is enabled because the Redirection on No Answer feature and Force Answer are mutually exclusive. If both are defined, Auto-answer takes precedence over Redirection on No Answer.

**Step 2** Using Unified CVP Operations Console, configure the Unified CVP ring-no-answer timeout value.

This step causes Unified CVP to issue a requery to the system software, if the assigned agent does not answer. In CVP Operations Console, use the SetRNATimeout command to set the ring-no-answer timeout to a duration that is two seconds longer than the Redirection on No Answer time set in Step 1.

**Note** Set this timeout to under 30 seconds because the system software waits 30 seconds for Unified CVP to return a routing label and then fails, so Unified CVP needs to requery before this happens.

**Step 3** Using the Script Editor, account for requeries in the routing script to handle Redirection on No Answer situations.

Use the Target Requery script feature.

**Note** Do not create and schedule a new Routing script for Redirection on No Answer purposes in Unified CVP deployments.

Allows you to report on Redirection on No Answer information. This script enables Requery (selects the **Requery** check box) on the node in the script that selects and delivers the call to the first agent. Depending on the type of node used, the Requery mechanism selects a new target from the available agents or requires additional scripting.

For information about how Requery works for the different nodes, see *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*.

**Important** This script queues the call at the highest priority in the skill group(s) defined within the call variables. Otherwise, the call is no longer the first in queue, as it was when it was first assigned to the (unavailable) agent.

**Note**

- If you configure the Redirection on No Answer timer in the Unified ICM agent desk settings, it is not necessary to configure the Unified CM Call Forward No Answer fields for the agent extensions in the Unified CM configuration. To configure them for cases when an agent is not logged in, set the Unified CM system service parameter for the Unified CM Call Forward No Answer timer at least 3 seconds higher than the Unified ICM Redirection on No Answer timer on each of the Unified CM nodes.
- To ensure that Redirection on No Answer calls adversely affect the service level, define the service level threshold to be less than the Redirection on No Answer timer at the call type and service.

# Configure Automatic Wrap-Up

Automatic wrap-up allows you to force agents into Wrap-up mode when they are finished with inbound or outbound calls.

**Procedure**

**Step 1** Select **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Desk Settings List**.

Use these two fields to enable automatic wrap-up:

- Work mode on Incoming
- Work mode on outgoing

Choose either **Required** or **Required with wrap-up data** to indicate automatic wrap-up.

Also, enter the time, in seconds, allocated to an agent to wrap-up a call.

**Step 2** Configure agent desk settings to require appropriate Reason Codes.

This configuration allows you to determine if and when agents are required to enter a Reason Code when they log out or enter a Not Ready state.

**Step 3** Agent should log out and then log in to the Finesse Agent Desktop, for any change, you perform in **Agent Desk Settings** to take effect.

# Configure Supervisor Assist and Emergency Alert

**Procedure**

**Step 1** Configure agent desk settings by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Desk Settings List**.

This step allows you to define the following:

- Assist call method

- Emergency alert method

**Step 2** Set up the call type by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Call Type List**

This step allows you to set up the call type and associate it with the dialed number and the routing script.

**Step 3** Configure Dialed Number for supervisor by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Dialed Number/Script Selector List**.

This step allows you to define the following:

- Dialed number string
- Call type

**Step 4** Configure Agent Team by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Team List**.

Allows you to define the Supervisor script dialed number option.

**Step 5** Using the Script Editor, create a routing script to associate the dialed number.

Use the Agent to Agent node to route the call to the primary supervisor by editing the formula with the call preferredagentid. In addition, in case this routing fails, set up a route to the skill group or precision queue where the secondary supervisors are located.

This step allows you to report on blind conference and consultative call information. This script associates the supervisor's dialed number with the script using the Script Editor's Call Type Manager window.

For more information about agent desk settings, agent teams, and dialed numbers, see Cisco Unified Contact Center Enterprise Installation and Upgrade Guide and the Configuration Manager online help.

# Unified CCE Administration Supervisor Access and Permissions

Supervisors can use Unified CCE Administration to manage skill group membership and attributes for the agents whom they supervise. Supervisors can change the passwords of agents who are not enabled for single sign-on. In Unified CCE Administration tools, supervisors can see the skill groups and teams that are configured on their peripherals.

**Note** The Unified CCE Administration web tool assumes that you are connecting with the primary AW. If you connect with the secondary AW, you see errors when saving configuration changes.

Sign in to Unified CCE Web Administration, at `https://<IP Address>/cceadmin`. *<IP Address>* is the address of the AW-HDS-DDS.

Supervisors on an IPv6 network sign in to Unified CCE Administration at `https://<FQDN>/cceadmin`. *<FQDN>* is the fully qualified domain name of the AW-HDS-DDS.

The format of a fully qualified domain name is hostname.domain.com.

When single sign-on is enabled, supervisors should use the password configured with their SSO identity provider. When single sign-on is disabled, they should use the password entered in the UCCE agent configuration.

If supervisors are enabled for single sign-on, after entering their username they are redirected to the Identity Provider sign-in screen to enter their credentials. Supervisors are redirected to Unified CCE Administration after successfully signing in.

**Note** Cisco Unified CCE supports SAM Account Name and User Principal Name format for supervisor login name configuration. However, Finesse supports *only* User Principal Name (UPN). Therefore, use only the UPN login format for configuring the non-SSO EA (Enterprise Agent) Supervisor login name.

Supervisors can access tools on the Manage menu, as follows:

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

| Tool | Permissions |
|---|---|
| Skill Groups | On the Skill Group List page, supervisors can see and edit membership for skill groups. Supervisors cannot add or delete skill groups.<br>• **General** tab: Fields are read-only.<br>• **Members** tab: Supervisors can add and remove skill groups for agents that they supervise. |
| Teams | Read-only. |

For more information about using the Unified CCE Administration tools, see the online help.

# Network Transfer for IVR Configuration

## Configure Network Transfer from IP Phone

To configure network transfer from an IP Phone, complete the following steps.

**Procedure**

**Step 1** Define a CTI Route Point, for example “9999”, in the Unified CM. Associate it with the JTAPI User that is connected to the Unified ICM/CCE PIM in the system software.

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

**Step 2** In the Administration Client or Administration & Data Server, define a Dialed Number for the Unified ICM/CCE PIM and a call type for that dialed number. You can then associate this call type with a Unified ICM/CCE script; for example, “NetXfer2.”

**Note** Do not define the labels of agents for the Unified CM PG. Instead, define the labels for the VRU PIM so that the route result is returned to VRU instead of a Unified CM PG. If you do define the agent labels for the Unified CM PG, the Router returns the route result to the VRU PIM, if “Network Transfer Preferred” is enabled on the Unified CM PG and VRU PIM and returns the route result to the Unified CM PG if “Network Transfer Preferred”" is disabled on the Unified CM PG and VRU PIM.

**Step 3** When the call is delivered to Agent 1 using the Unified ICM/CCE Script “NetXfer1,” the agent can dial the number 9999 to send the call to another script, “NetXfer2.”

## Configure Network Transfer from Agent Desktop

To configure network transfer from an agent desktop, complete the following steps.

### Procedure

**Step 1** Define a “Dialed Number Plan” in the system software. The routing client is the Unified ICM/CCE PIM and the dialed number is the one defined before for the Unified ICM/CCE PIM.

**Step 2** Set the Post Route to **Yes** and the Plan to **International**.

**Step 3** In the agent desk settings, select all the **Outbound access** check boxes.