Administration Guide for Cisco Unified Contact Center Enterprise, Release 12.5(1)

First Published: 2019-02-07

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

Preface

Change History

This table lists changes made to this guide. Most recent changes appear at the top.

Change	See	Date
Added support to scale to 36000 Agents from 24000 Agents Reference Design	Change Limits for Calls Per Second to Support 36000 Agents	February, 2021
Initial Release of Document for Release 12.5(1)		February, 2020
Added support for Cloud Connect	About Cloud Connect	
Added support for Smart Licensing	Smart Licensing	

About This Guide

This guide explains how to interpret reporting data that is stored in, and retrieved from, the Cisco Unified Contact Center Enterprise (Unified CCE) Unified Contact Center Enterprise database. This guide also helps you understand the importance of planning, configuration, and scripting for accurate reporting data.

Audience

This guide is written for anyone who uses Cisco Unified Intelligence Center (Unified Intelligence Center) to generate reports using the stock Cisco reporting templates. Stock templates are Cisco templates that are

installed with the reporting application, that are populated from the Unified CCE database, and that are qualified by Cisco Systems, Inc.

Contact center supervisors and administrators who are responsible for configuring and scripting Unified CCE will also find this guide useful.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Field Notice

Cisco publishes Field Notices to notify customers and partners about significant issues in Cisco products that typically require an upgrade, workaround, or other user action. For more information, see *Product Field Notice Summary* at https://www.cisco.com/c/en/us/support/web/tsd-products-field-notice-summary.html.

You can create custom subscriptions for Cisco products, series, or software to receive email alerts or consume RSS feeds when new announcements are released for the following notices:

- Cisco Security Advisories
- Field Notices
- End-of-Sale or Support Announcements
- Software Updates
- Updates to Known Bugs

For more information on creating custom subscriptions, see *My Notifications* at https://cway.cisco.com/mynotifications.

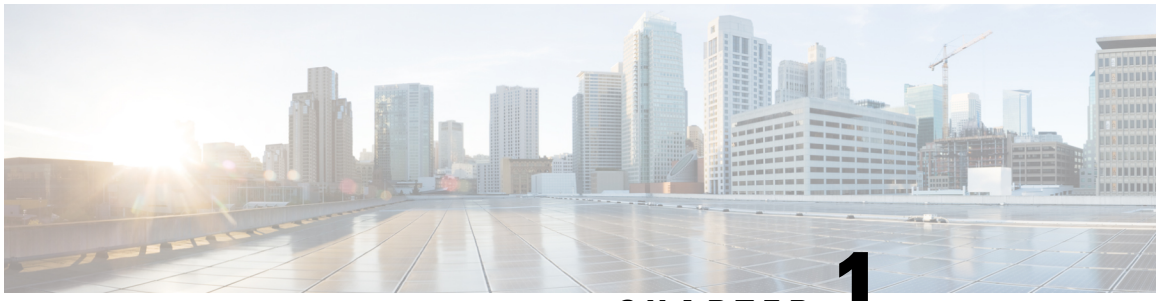
Documentation Feedback

To provide comments about this document, send an email message to the following address: contactcenterproducts_docfeedback@cisco.com

We appreciate your comments.

PART I

Agent Management and Call Routing



CHAPTER 1

Cisco Unified Contact Center Enterprise Agents

Add Users to Local Security Group

Configuration users can configure Agents, Supervisors or Teams and perform other configurations only after they are added to the `UcceConfig` group on the local machines.

You need to add the Unified CCE configuration users to the `UcceConfig` group in all the local Distributor machines.

Procedure

Step 1 Click **Server Manager** > **Tools** > **Computer Management**.

Step 2 Select **Local Users and Groups**.

Step 3 Double-click **Groups**.

Step 4 Right-click **UcceConfig**. Select **Properties**.

Step 5 Click **Add** and enter the user name in the **Edit the object names to select** text box. Click **Check Names** to validate the user name.

Step 6 After the user name is successfully validated, click **OK**.

Step 7 Click **Apply** and **OK** in the **Properties** dialog box.

Step 8 Close the **Computer Management** and **Server Manager** windows.

Agent Administration

This section provides information about the Unified CCE agent, including associating the agent with database records and agent desk settings.

Agents

An agent is an individual who handles customer contact within your contact center. In a Unified CCE configuration, you can create two types of agents:

Agent type	Description
Voice-only agents	Agents can receive telephone calls. You can also configure voice-only agents to receive non-voice requests such as chat and email.
Multichannel agents	Agents can receive voice calls and requests from other media. You can also configure multichannel agents to *only* receive non-voice requests such as chat and email. **Note** You must have Cisco multichannel software installed as part of your Unified CCE configuration to create multichannel agents.

Note In most cases, the Cisco Unified Communications Manager (Unified CM) peripheral on the Generic CUCM peripheral gateway (PG), which is set up with your initial Unified CCE installation, tracks and records the state and activity of all voice and non-voice agents. You can configure a non-voice PG rather than a Unified CM PG to monitor state and activity of agents configured as non-voice agents. However, this is optional, and is not necessary if you have a Unified CM peripheral on the Generic CUCM PG.

Database Records for Voice-Only Agents

In the Unified ICM database, you must associate each agent with two database records.

Unified ICM database record	Description
Person record	Identifies the individual. Person records must exist for all Unified CCE agents. Every agent in your configuration must have a single Person record. You can then associate this record with one or multiple Agent records, as described below.
Agent record	Identifies the agent working on a particular peripheral. There must be a one-to-one correspondence between each Agent record and its associated peripheral. However, in Unified CCE, if an agent is going to be working on several peripherals, you can create several Agent records and associate these with the same Person record. In this way, a single agent can work on several different peripherals.

When you create an Agent record, you have the option of associating it with an existing Person record (select **Select Person**). If you do not associate the Agent record with an existing Person record, a new Person record is automatically created when you create the agent.

Before you assign an agent as a supervisor, ensure that the agent has an Active Directory account.

Database Records for Multichannel Agents

Unified CCE agents who use multichannel software are associated with three different database records:

- The Person record in the ICM Unified CCE database
- The Agent record in the ICM Unified CCE database
- The Agent record in the database for the multichannel application

Agent Desk Settings Configuration

You must associate each Agent record with an *agent desk setting.* You use the agent desk settings configuration to associate a set of permissions or characteristics with specific agents. These settings are comparable to Class of Service settings on a PBX or ACD. Desk settings are associated with an agent when the agent is configured in the Unified ICM database. The desk settings are global in scope and you can apply them to any configured agent on any peripheral within an ICM Unified CCE configuration.

If desktop settings are not associated with a configured agent, the agent is assigned the peripheral default settings. The peripheral default settings depend on the default setting for the Generic CUCM PG the agent is logged in to.

Related Topics

Agent Feature Configuration with Agent Desk Settings List Tool, on page 7

Using Multichannel Gadgets in Cisco Finesse

The Agent is logged into both voice and multichannel Media Routing Domains in Cisco Finesse desktop using the multichannel gadgets and the Agent is also configured for Logout non-activity time in the Unified CCE Agent Desk Settings Configuration.

In this scenario, if the Agent is idle, which means the Agent is Not Ready in the Voice Media Routing Domain, the Peripheral Gateway logouts out the Agent from the voice Media Routing Domain after the configured Logout non-activity timer has elapsed. The Cisco Finesse desktop closes the Agent's session and this terminates the Agent's multichannel Media Routing Domain session, although the Agent may be actively working on a multichannel task.

As a result, the Agent's multichannel Media Routing Domain state and tasks state both are remained in the same state before the Agent logged out of voice Media Routing Domain.

To work on the multichannel Media Routing Domain tasks, agent has to login again to Cisco Finesse desktop.

Note Do not configure Logout non-activity time in Unified CCE Agent Desk Settings configuration, if you are using the Cisco Finesse desktop to login Agents in both voice and multichannel gadgets as mentioned above.

Agent Teams and Supervisors

You can organize Unified CCE voice agents into *teams*. A team is a collection of agents grouped for reporting purposes.

Note A single agent can belong to only one team.

Unified ICM/CCE software allows you to group individual agents into agent teams that supervisors can manage. Agent teams are assigned to a specific peripheral, so you must assign all agents of a given team to the same Unified CM peripheral.

Unified ICM/CCE software lets you assign both Primary and Secondary supervisors to an individual team; set up your teams with both a Primary and a Secondary supervisor. This setup helps to accommodate Supervisor and Emergency assist scenarios.

Supervisors listed on the agents team list are able to view real-time statistics (using your reporting application). Supervisors can, for example, barge-in, intercept, silently monitor, and log out agents in the associated team.

For reporting purposes, you can report on agent teams and agents grouped into teams. Also, supervisors can run reports on their teams. (For more information about reporting, see Cisco Unified Contact Center Enterprise Reporting User Guide.)

Each team you set up must have an agent supervisor associated with it. You can then configure supervisory agent features, to allow the supervisor to improve monitor agent activity and assist agents on their team. When you create an agent supervisor, you must enter the following information for the supervisor:

- Windows Domain name to which the agent team belongs
- Windows User ID for the supervisor
- Windows password for the supervisor

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

- An agent can be a member of only one agent team.
- An agent team can have only one Primary Supervisor.
- A supervisor can be a supervisor of any number of agent teams.
- A supervisor for an agent team can also be a member of that agent team.
- All agents belonging to an agent team and all supervisors for that agent team must be on the same peripheral.
- A supervisor cannot be using the Windows administrator account when logging in as supervisor.

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

Agent teams and Multichannel Applications

You can group voice agents into teams using the Unified ICM/Unified CCE Administration User Interface. However, there is no team feature in Enterprise Chat and Email; therefore, you cannot group Enterprise Chat and Email agents into teams.

For more information about supervisory features, see *CTI OS System Manager Guide for Cisco Unified ICM*.

Related Topics

Desktop Feature Config, on page 7

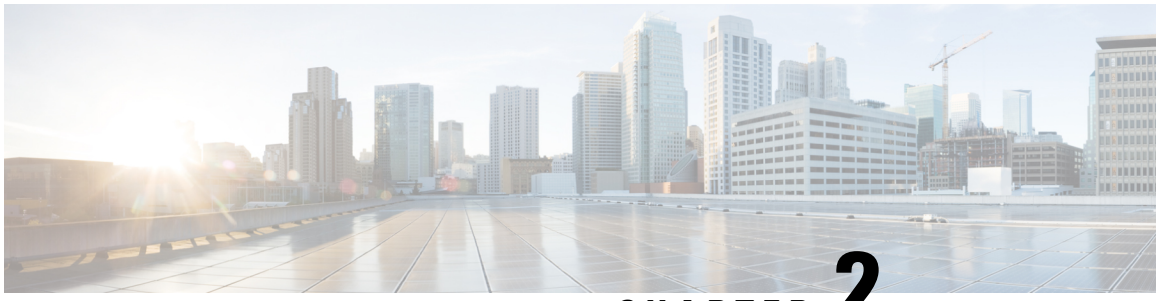
Single-Line Versus Multi-line Behavior

The following table details single-line behavior versus multi-line behavior.

Action	Single-line behavior	Multi-line behavior
Accept a routed call while call is on second line?	Yes	Yes, when Non ACD Line Impact is set no impact for the deployment.
Supervisor Monitor using Unified CM-based silent monitor	Yes	Yes. **Note** Non-ACD lines do not support Unified CM-based silent monitoring.
Call park	Supported on unmonitored second line	Not supported because all lines are monitored.
Join Across Lines (JAL)/Direct Transfer across Lines (DTAL)	Not supported	**Note** Use of JAL and DTAL phone features is deprecated. Do not use these features in new deployments.
Shared line	Supported on unmonitored line; no configuration limitations	Supported on non-ACD lines. Sign-in is allowed for only one agent on a shared extension when shared lines exist between multiple devices.However, one agent can have two phones that share a second common line. The agent cannot sign into both phones at the same time. Unified CCE does not support shared lines for ACD lines.
Call Waiting / Busy trigger > 1	Supported with caveats. For more information, see the section *Direct Agent Dialing* in the *Solution Design Guide for Cisco Unified Contact Center Enterprise* https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html	State Agent Login rejected if Busy trigger is not 1, and max calls is not 2 for each of the non-ACD lines.

Action	Single-line behavior	Multi-line behavior
Reporting on second line calls	Use CDRs in Unified CM	Termination Call Detail Records for call to or from an agent's Non ACD line with an unmonitored device or another agent's Non ACD line is reported with a Non ACD Peripheral Call Type. Reporting for all calls on the Non ACD line is captured in the Agent Interval table for that agent.
Number of configured lines on phone	No limit described (only monitoring one line)	Maximum of four lines. Agent login will be rejected. Config Alert generated.

For more information about enabling the Cisco Round Table phones, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*. For more information about configuring the Cisco Round Table phones, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* and the Cisco Unified Communications Manager documentation.



CHAPTER 2

Desktop Feature Config

Agent Feature Configuration with Agent Desk Settings List Tool

You must associate each voice Agent record with an *agent desk setting* (not necessary for non-voice agents). You can use the agent desk settings list tool configuration to associate a set of permissions or characteristics with specific agents. You can use the agent desk settings list tool to configure the following agent features:

- Agent Wrap-up
- Reason Codes
- Redirection on No Answer
- Emergency and Supervisor Assist Calls

Note In Parent/Child deployment type, the agent name is automatically configured for the customer. Spaces are not allowed in agent IDs. In a specific scenario, if a child agent is created with a space or a "-", in either the First Name or Last Name field, the name are not created on the parents.

Note For any change, you perform in the **Agent Desk Settings** to take effect, log out and then log in to the Finesse Agent Desktop.

Agent Wrap-Up

Agents can enter Wrap-up mode after completing a call. Wrap-up mode enables the agent to finish with any tasks that require after-call work before entering a Ready state. When in Wrap-up mode, the agent is not routed any additional tasks.

Agents can manually enter Wrap-up state by activating the wrap-up button on their soft phone. You can also configure agent desk settings so that agents automatically enter Wrap-up mode after finishing each call.

When you create agent desk settings using the Unified ICM/Unified CCE Administration User Interface, you can specify whether agents enter Wrap-up mode automatically after finishing incoming calls. The Work Mode Settings allow you to specify whether the agent must enter Wrap-up mode after incoming calls. You can also use these settings to require agents to enter reason codes while in Wrap-up mode (incoming calls only).

Reason Codes

Agents select Reason Codes when they:

- Log out of the agent desktop system
- Enter Wrap-up mode after a call
- Change to a Not Ready state

Reason Codes allow you to track the agent's state and logout status as it changes. You configure Reason Codes using the agent desktop application.

Agent Desk Settings That Affect Reason Codes

Agent desk setting option	Affects this type of reason code
Work mode on Incoming	Wrap-up
Idle reason required	Not Ready
Logout reason required	Logout

Wrap-Up Reason Codes and Work Mode

If you use the agent desktop, you can use the Work Mode on Incoming option on the agent desk settings list window to specify when and if agents are required to enter Reason Codes when entering Wrap-up for incoming calls. The following table describes Work Mode on Incoming options and explains how Reason Codes are related to each.

Work Mode	Description	Reason Code
Required	Ensures that the agent automatically enters Wrap-up state after completing the call.	The agent can choose to enter a Reason Code.
Optional	Allows agents to choose whether to activate the wrap-up button or the **Not Ready** button at the end of the call.	If the agent uses the wrap-up button, the agent can choose to enter a Reason Code.
Not Allowed	Restricts the agent from entering Wrap-up mode. The agent can go into Not Ready mode.	The agent can decide whether to enter a Not Ready Reason Code.

Work Mode	Description	Reason Code
Required with wrap-up data	Ensures that the agent automatically enters Wrap-up state after completing the call. **Note** This mode is not supported for outgoing calls.	The agent must enter a Reason Code.

Predefined Reason Codes

Unified CCE uses several predefined reason codes to indicate certain system events, described in the following table.

Reason Code	Description
32767	Agent state changed because the agent did not answer the call.
50001	The CTI client disconnected, logging the agent out. **Note** This reason code is converted to a 50002, so 50001 does not display in the agent log out records.
50002	A CTI component failed, causing the agent to be logged out or set to Not Ready. This could be due to closing the agent desktop application, heartbeat time out, a CTI Server failure, or CTI server client failure (like Finesse.)
50003	Agent was logged out because the Unified CM reported the device out of service.
50004	Agent was logged out due to agent inactivity as configured in agent desk settings.
50005	For a Unified CCE agent deployment, where the Agent Phone Line Control is enabled in the peripheral and the Non ACD Line Impact is configured to impact agent state, the agent is set to Not Ready while talking on a call on the Non ACD line with this reason code.
50010	Agent was set to Not Ready state because the agent was routed two consecutive calls that did not arrive.
50020	Agent was logged out when the agent's skill group dynamically changed on the Administration & Data Server.
50030	If an agent is logged in to a dynamic device target that is using the same dialed number (DN) as the PG static device target, the agent is logged out.
50040	Mobile agent was logged out because the call failed.
50041	Mobile agent state changed to Not Ready because the call fails when the mobile agent's phone line rings busy.
50042	Mobile agent was logged out because the phone line disconnected while using nailed connection mode.
-1	Agent reinitialized (used if peripheral restarts).

Reason Code	Description
-2	PG reset the agent, usually due to a PG failure.
-3	An administrator modified the agent's extension while the agent was logged in.

These reason codes appear in these reports:

- Agent log out reports if the event caused the agent to log out.
- Agent real time reports if the agent was set to a Not Ready state.
- Agent Not Ready reports.

Important For reporting on all PGs other than VRU PGS, be sure to select the **Agent event detail** check box on the Agent Distribution tab in the Unified ICM/Unified CCE Administration User Interface's PG Explorer tool. You must select this check box to report on Not Ready Reason Codes.

Redirection on No Answer

You can configure your Unified CCE system to handle and accurately report on situations when the agent does not answer their phone. These situations are referred to as Redirection on No Answer.

Although you can specify some values that control Redirection on No Answer situations, configuring Redirection on No Answer involves additional steps:

- Unified ICM/Unified CCE configuration
- Unified ICM/Unified CCE scripting
- Unified CM configuration

Redirection on No Answer conditions are handled by two routing scripts: the initial routing script and a script specifically set up for these conditions. The initial routing script handles the incoming call; when the call is redirected on no answer from the agent's IP phone, the script branches to another script set up specifically for Ring No Answer conditions. For more information on Redirection on No Answer, see the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html.

Note The Target Requery script feature, implemented using the Label, Queue, Route Select, and Select nodes, is not supported for Unified CCE systems; however, it is supported for Cisco Unified Customer Voice Portal (Unified CVP).

Emergency and Supervisor Assist Calls

Agents can activate Supervisor Assist or Emergency Assist buttons on their desktop when they need special assistance from the primary or secondary supervisor assigned to their team.

Agents can use the Supervisor and Emergency assist features, regardless of whether or not they are on a call.

There are two types of Supervisor and Emergency Assist calls:

- Existing call—Consult must be selected as an option on the agent desktop settings for supervisor or emergency assist. If the agent is on a call when they activate either the supervisor or emergency assist feature on their desktop, the CTI software activates the conference key on behalf of the agent's phone and calls the supervisor via the Supervisor or Emergency Assist script. (This example assumes the emergency or supervisor assist script has an Agent-to-Agent node to find a supervisor.) The supervisor answers the call and consult privately with the agent. During the consultation, the supervisor can decide to barge into the call.
- No call—If the agent is not on a call when they activate either the supervisor or emergency assist feature on the agent's desktop, the CTI software activates the make call functionality on behalf of the agent's phone and calls the supervisor via the Supervisor or Emergency Assist script.

Note Blind Conference is not supported for Emergency and Supervisor Assist.

Agent Reskilling

Unified Contact Center includes the CCE web Administration application, which is a browser-based application and is separate from the supervisor desktop. CCE web administration lets supervisors change the skill group designations of agents on their team, quickly view skill group members, and view details on individual agents.

Note
- If an agent is currently in a call, a change to the agent's skill group membership takes place after the call has terminated.

Related Topics

Managing Agents, on page 66

Skill Groups and Precision Queues per Agent Limit

Unified ICM and Unified CCE impose a default limit on the number of skill groups and precision queues that you can assign to a single agent. After this limit is reached, you cannot reassign additional skill groups or precision queues.

You can also use the Configuration Limit tool to specify your own limit on the number of skill groups and precision queues that you can assign to an agent. For optimum performance, you can specify a limit far lower than the system default.

For more information, see the *Dynamic Limits for Skill Groups and Precision Queues Per Agent* topic in the *Solution Design Guide for Cisco Unified Contact Center Enterprise, Release 12.5(1) and later* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-implementation-design-guides-list.html

Caution The Configuration Limit tool is a command-line tool utility from the bin directory of all Unified ICM and Unified CCE Administration & Data Servers. Access is limited to users with privileges for Config Users for the chosen customer instance. For more information about the Configuration Limit tool, see *Outbound Option Guide for Unified Contact Center Enterprise*.

Modify the Precision Queues and Skill Groups per Agent Limit

Complete the following steps to view and modify the current limit on the precision queues per agent and skill groups per agent using the Configuration Limit tool:

Procedure

Step 1 From the Windows menu, select **Start** > **Run**, type **`configlimit`** , and then click **Enter**.

Note Run the Configuration Limit tool on the same machine as the Distributor for the instance you want to configure. If more than one instance of the Administration & Data Server is installed on the Distributor machine, use the Select Administration Server tool to select the instance you want to configure.

Step 2 To view the current configuration limit, run the following command:

```
cl /show
```

Step 3 To change the current limit, enter a command in the following format:

```
cl /id 1 /value [ConfigLimitCurrentValue] [/update]
```

Where:

- id 1 = the ID of the skill groups/precision queues per agent limit.
- ConfigLimitCurrentValue = the parameter limit. In this case, the parameter limit applies to both the skill groups per agent and the number of precision queues per agent.

For example, to change the precision queues/skill groups per agent limit to 50, enter the following:

```
cl /id 1 value/50 /update
```

Note Using the Configuration Limit tool, you can change the ConfigLimitCurrentValue only. You cannot change the ConfigLimitDefaultValue.

Additional Requirements

Lowering the Limit

If you have modified the skill groups per agent limit to be lower than the system default, no additional changes are necessary. The new, lower limit is enforced immediately. Note that the new limit does *not* impact agents

whose existing skill group membership exceeds the new limit until the next attempt to add a new skill group for those agents. At that time the new limit is enforced, preventing you from adding additional skill groups.

Exceeding the Default Limit

If you have modified the skill groups per agent limit to be higher than the system default (in spite of the Warning given above), certain deployments require additional changes (listed in the following sections) to your system to use the new limit and allow you to add additional skill groups.

IPCC Gateway PG

For IPCC Gateway deployments, modify the following registry keys on your IPCC Gateway PGs to include the new value. A change to the registry requires that you restart the PG service.

IPCC Enterprise Gateway PIM (Cisco Unified Contact Center Enterprise parent):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance
>\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim{m}\ACMIData\Config\MaxSkills
```

IPCC Express Gateway PIM (Cisco Unified Contact Center Express parent):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\< customer_instance
>\PG{n}[A|B]\PG\CurrentVersion\PIMS\pim{n}\ACMIData\Config\MaxSkills
```

Network Transfer for IVRs

When a call is transferred from an IVR (for example, IP IVR) to an agent and that agent wants to transfer the call to another agent, the transfer can be made either from the agent's IP phone or the agent desktop.

Transfers made from the:

- IP phone are made using CTI route points that point to a Unified ICM/Unified CCE script.
- Agent desktop are made using the Dialed Number Plan.

Note If the route point is configured using Unified CM, there is no difference between using the hard phone or the desktop phone.

For network transfer from either the IP phone or the agent desktop, you must queue the call to the skill group in the first Unified ICM/Unified CCE script; for example, “NetXfer1,” to create the call context. In this script you must set the “networkTransferEnabled” flag to “1”.

Note IP IVR *does not* support network transfer. Unified CVP supports *only* network “blind” transfer.

Unified CCE Routing

To understand how Unified CCE routes voice calls, you must understand the concepts of routing operation and routing configuration.

Routing Operations

To understand how Unified CCE routing occurs, you must understand these concepts:

- **The Routing Client:** The Unified CCE component that submits a route request to the Central Controller.

  In Unified CCE configurations, the routing client can be:

  - The Unified CM PG
  - An interexchange carrier (IXC)
  - A VRU PG
  - A Media Routing Peripheral Gateway

  When a routing client makes a request for a route from the Unified ICM/Unified CCE platform, it receives the response and delivers the call to the specified destination. If an Unified CCE agent is available, Unified ICM/Unified CCE software routes the call to the device target (phone) on the Unified CM (device targets are dynamically associated with the agent when the agent logs in to the system). If an agent is not available, you can configure Unified ICM/Unified CCE software to queue the call to IP IVR or Unified CVP.

- **Route and Queuing Requests:** Messages sent from the routing client to the Central Controller. Route requests typically pass along call detail information about the incoming call. Unified ICM/Unified CCE software uses information in the route request to determine which routing script is run for the call.

  Call detail information sent with the route request can include:

  - Dialed Number (DN)
  - Calling line ID (CLID)
  - Caller Entered Digits (CED)

  Queueing requests are messages sent from the VRU using the Cisco Service Control Interface. The VRU makes a queue request to provide announcements or music when no Unified CCE agents are available to take the call.

- **About Routing to the VRU with Unified CCE:** With Unified CCE you can ensure that voice calls are routed to the VRU when an agent is not immediately available. The call is queued to the VRU and sent to the next available agent via the routing script.

  The configurations for routing to a VRU in a Unified CCE environment include:

  - Translation Route to the VRU via a route on the PG. The Unified CM uses the DNIS in the translation route to direct the call to the VRU.
  - A network route request is issued by the carrier via the NIC. The DNIS and/or Correlation ID is retrieved from the carrier.

- The call is sent directly to the VRU, so that caller entered digits (CED) can be collected.

You do not need a translation route to a Unified CM PG because it is targeting agents and implicitly matches call data.

- **Routing a Call to the VRU:** Translation routing is the preferred method of routing a call to the VRU. The DNIS used in the translation route is not the original number dialed by the customer, but rather, the Dialed Number used to route the call to the VRU.

  The scenario is as follows:

  - Call comes in to the Unified CM.
  - Unified CM identifies the number as a route point for the Unified CM PG.
  - The Unified CM PG receives a route request from the Unified CM and forwards it to the CallRouter.
  - The CallRouter runs the script for the translation route to the VRU.
  - A Label is returned to the Unified CM via the Unified CM PG.
  - The Unified CM routes the call to the VRU, based on the CTI route point for the translation route.
  - VRU sends up a request instruction with the DN as the DNIS.
  - VRU PG matches up the call and the Correlation ID, then informs the CallRouter of the call arrival with a “request instruction.”
  - The CallRouter matches the correlation ID and finds the pending script/call.
  - The CallRouter continues with script (for example, run script).

    For translation routing, the VRU Type to configure in the Network VRU in the Unified ICM/CCEho Administration User Interface is type 2.

    Be sure the Unified CM PG routing client and the VRU PG routing client both have the labels mapped for the peripheral targets in the translation route.

Routing Configuration

To set up routing in your Unified CCE system, you must set up the following entities:

- **Dialed Numbers:** The dialed number is the number that the caller dials to contact an agent. It is sent as part of the call detail information in the route request message sent from the routing client.

  In the system software, you set up a Dialed Number List. It identifies all of the phone numbers in your contact center that customers can dial to initiate contact.

  The Dialed Number plays an integral role in routing calls. Dialed Numbers are required pieces of Unified ICM call types that are used to identify the appropriate routing script for each call.

- **Call Types:** A call type is a category of incoming Unified ICM routable tasks. Each call type has a schedule that determines which routing script or scripts are active for that call type at any time. There are two classes of call types: voice (phone calls) and non-voice (for example, email and text chat). Voice call types are categorized by the dialed number (DN), the caller-entered digits (CED) and the calling line ID (CLID). Non voice call types are categorized by the Script Type Selector, Application String 1, and Application String 2. In either case, the last two categories of the call type can be optional. For voice

call types, the caller-entered digits and the calling line ID can be optional, depending on the call. For non voice call types, Application String 1 and Application String 2 can be optional, depending on the application.

Because the call type determines which routing script is run for a call, the call type defines call treatment in a Unified CCE system. Therefore, the call type is the highest level reporting entity. Reporting on call type activity provides insight into end-to-end customer interactions with the system and with agents by providing data such as service level adherence, transfers, average speed of answer, calls handled, and calls abandoned.

In routing scripts, such as scripts for Self-Service VRU applications, you may change the call type at specific points in the script to indicate that a transaction has been completed. For example, if the customer is calling a bank and successfully checks their account balance using a Self-Service script, you may want to change the call type to indicate that the account balance transaction has completed and a new transaction has begun.

You can also change the call type in a script to invoke a new routing script associated with that call type. For example, if a call is not answered at an agent's desktop, you can change the call type in the script to redirect the call to a different script designed for Redirection on No Answer. The Redirection on No Answer script assigns a different agent to handle the call.

- **Routes:**Unified ICM/Unified CCE software uses routes to define the mapping of a target to a specific label for a routing script. Targets include services (service targets), skill groups (skill targets), agents (device targets), and translation routes.

  Routes must be defined for VRU Translation Routing and to route calls to agents.

- **Device Targets:** Device targets are deprecated. A device target is a telephony device that can be uniquely addressed (or identified) by a telephone number. A device target is not associated with any one peripheral. Each device target must have one or more labels associated with it, although only one label may exist per routing client. Replace device targets with **Agent Targeting Rules**, which greatly simplifies call routing configuration.

- **Labels:** A label is the value that Unified ICM/Unified CCE software returns to a routing client instructing it where to send the call. The routing client can map the label to an announcement, a trunk group and DNIS, or a device target. Special labels might instruct the routing client to take another action, such as playing a busy signal or an unanswered ring to the caller.

  If the label is for a device target, the routing client is responsible for delivering the call to the device target on the Unified CM through the voice gateway.

  If the label is for a VRU queue point, the routing client delivers the call to the Route Point on the VRU. The VRU must recognize that the call has arrived and then request queue instructions from Unified ICM/Unified CCE software. Unified ICM/Unified CCE software returns either a destination for the call or instructions on what script the VRU will run, based on a particular Call Type.

- **Services:** You set up Services in Unified ICM/Unified CCE software to represent the type of processing that a caller requires, and to configure VRU Services to route calls to the VRU. For example, you might define separate services for Sales, Support, or Accounts Payable. A Service is often associated with a peripheral and can be referred to as a Peripheral Service.

  For Services that are used to route a call to an agent, you must associate them with skill groups. You associate different Skill Groups with Services by making them members of the Service. Using Services allows you to group agents working in like skill groups.

- **Skill Groups:** Agents must be associated with skill groups to receive Unified ICM-routed calls. You create skill groups using the Unified ICM/Unified CCE Administration User Interface.

A *base skill group* is the main skill group created using the Unified ICM/Unified CCE Administration User Interface. Using base skill groups ensures accurate agent reporting and simplifies configuration and scripting for your contact center.

Agents must be associated with skill groups or precision queues.

Note A *sub-skill group* is a subdivision of a base skill group. Sub-skill groups are not supported since Unified CCE 9.0(1); the only instance where they are still supported is for Avaya PG and Avaya Aura PG peripherals in Unified ICM deployments. You *cannot* create a sub-skill group for the System PG, CallManager, and ARS PG peripheral types. You can only remove sub-skill groups from these peripheral types. Sub-skill groups are also not supported for non-voice skill groups. You cannot create sub-skill groups for chat and email.

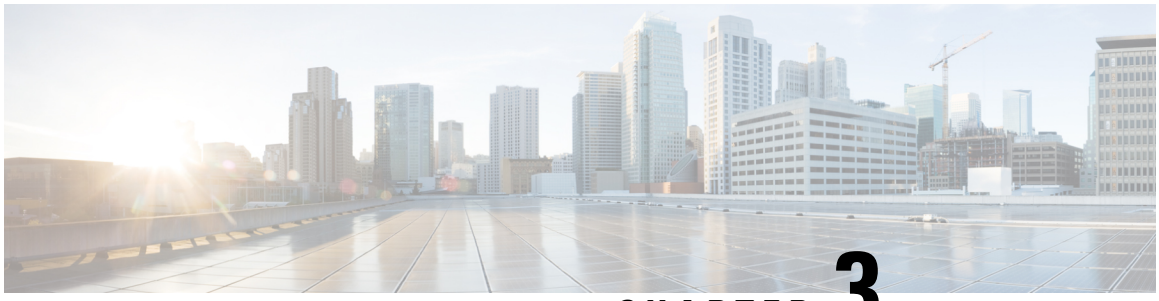
- **Precision Queues:** You can create multidimensional precision queues based on predefined business criteria using the Unified CCE Web Administration. Agents automatically become members of these precision queues based on their attributes, dramatically simplifying configuration and scripting.
- **Migrating from Sub-skill Groups to Base or Enterprise Skill Groups**

  Follow these steps to migrate from sub-skill groups to base and enterprise skill groups:

  - Disable the sub-skill group mask for the peripheral using the PG Explorer tool. All skill groups created after you complete this are base skill groups.
  - Define a new base skill group to correspond with each sub-skill group being removed.
  - Assign agents to the new base skill groups and remove them from your sub-skill groups.
  - Optionally, create enterprise skill groups to group the base skill groups.
  - Update all of your routing scripts and routing templates so that they refer to the newly created base or enterprise skill groups.

Routing Scripts

A routing script, created using the Script Editor, identifies the desired agent based upon skills and customer database profile, determines the call target, and returns a route response to the routing client.



CHAPTER 3

Routing Tasks Multichannel Options

Task Routing for Third-Party Multichannel Applications

Task Routing APIs provide a standard way to request, queue, route, and handle third-party multichannel tasks in CCE.

Contact Center customers or partners can develop applications using Customer Collaboration Platform and Finesse APIs in order to use Task Routing. The Customer Collaboration Platform Task API enables applications to submit nonvoice task requests to CCE. The Finesse APIs enable agents to sign into different types of media and handle the tasks. Agents sign into and manage their state in each media independently.

Cisco partners can use the sample code available on Cisco DevNet as a guide for building these applications (https://developer.cisco.com/site/task-routing/).

For information about configuring Task Routing for third-party multichannel applications, see the *Cisco Unified Contact Center Enterprise Features Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html.

Routing Unified Interaction Manager Tasks

Unified CCE Configuration for Multichannel Routing

To route contact requests submitted from the World Wide Web or email, you must configure:

- Media Routing Peripheral Gateway
- Media Routing Domains and Media Classes
- Multichannel agents
- Application instances
- Administration connections
- Multichannel skill groups

- Multichannel routing scripts

For more information about configuring Unified CCE for multichannel routing with Unified Interaction Manager, see the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Note When implementing Task Routing for third-party multichannel applications, some of the configuration in the list above is provided by default or automated. See the *Cisco Unified Contact Center Enterprise Features Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-feature-guides-list.html

Multichannel Software Configuration

After you complete your Unified ICM/Unified CCE configuration, you must configure your Unified ICM multichannel software.

The multichannel software you must configure includes Enterprise Chat and Email.

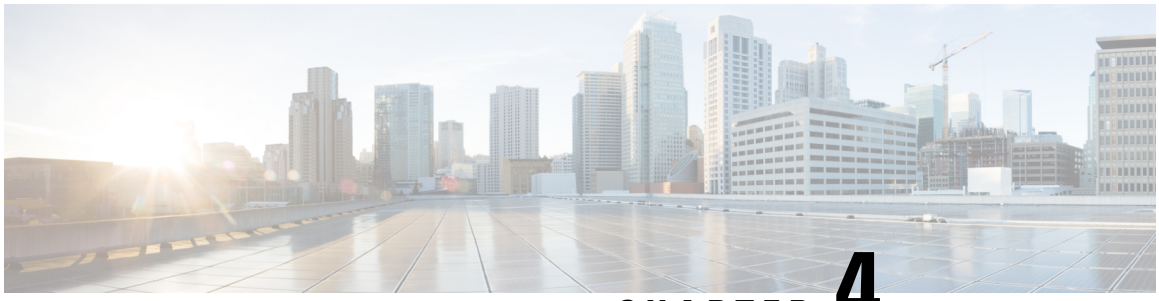
For more information about how to administer this component, see Enterprise Chat and Email Installation Guides and Administration Guides at

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-installation-guides-list.html, and

https://www.cisco.com/c/en/us/support/customer-collaboration/cisco-enterprise-chat-email/products-maintenance-guides-list.html.

PART II

Administrative Tasks with Cisco Unified Cisco Contact Enterprise



CHAPTER 4

Smart Licensing

Overview

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

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

You can use Smart Licensing to:

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

Related Topics

License Management, on page 40
Prerequisites for Smart Licensing, on page 25
Smart License Deployments, on page 25
Evaluation Mode
Smart Licensing Task Flow, on page 27
Obtain the Product Instance Registration Token, on page 28
Configure Transport Settings for Smart Licensing, on page 28
Select License Type, on page 29
Register with Cisco Smart Software Manager, on page 30
Registration, Authorization, and Entitlement Status, on page 32
Out-Of-Compliance and Enforcement Rules, on page 34
Smart Licensing Tasks, on page 40
Renew Authorization, on page 40
Renew Registration, on page 41
Reregister License, on page 41
Deregister License, on page 42

Smart Licensing Capabilities

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

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

Creating a Smart Account is easy and takes less than five minutes. Create a Smart Account on software.cisco.com.

Documentation Resources

Table 1: Documentation Resources

For	Go to...
Smart Licensing Prerequisites	Prerequisites for Smart Licensing, on page 25
Understanding the License consumption Calculation	License Consumption Calculation, on page 37
Migration to Smart Licensing	Migrate to Smart Licensing, on page 39
Smart Licensing tasks in CCEADMIN	Smart Licensing Task Flow, on page 27
Best Practices	Best Practices, on page 42

Prerequisites for Smart Licensing

The following are the prerequisites for configuring Smart Licensing:

- **Smart Licensing Enrollment**

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

- **Adoption of License Integration Strategy**

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

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

  For more information, see Smart License Deployments, on page 25.

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

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

     - `cd %CCE_JAVA_HOME%\bin`

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

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

Related Topics

Configure Transport Settings for Smart Licensing, on page 28
Smart License Deployments, on page 25

Smart License Deployments

There are two software deployment options for Smart Licensing:

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

Direct - Cisco Smart Software Manager (Cisco SSM)

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

Cisco SSM allows you to:

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

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

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

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

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

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

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

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

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

Cisco SSM On-Prem Configuration

Perform these steps to get the correct URL for the customer's environment:

1. Log in to the On-Prem CSSM GUI with your virtual account.

Note The URL for the interface is https://<hostname_or_fqdn_of_CSSM>:8443

2. Click **Smart Licensing** link and navigate to **Inventory > Production Instance Registration Tokens** and click **Smart Call Home Registration URL**. This opens a pop-up window with the URL in it.
3. Copy and paste this URL in the **CCE Smart Transport URL** field to create the link.

This link is created using the Cisco SSM On-Prem adminstration configuration and matches with the Cisco Smart Licensing CA signed certificate .

Contact the Cisco SSM administration team to know the user side URL to generate tokens. Ensure the name used in the **CCE Smart Transport URL** matches the certificate for the Server. For example; if Cisco SSM is configured with an IP in the admin side then the Smart Call Home URL must use the same IP in the URL. If Cisco SSM is configured with just the hostname then the URL must match the same hostname too.

4. If the SmartAgent.log shows and error, check the URL to ensure the hostname/IP address matches with the hostname/IP address in the certificate.

Smart Licensing Task Flow

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

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

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

Related Topics

Obtain the Product Instance Registration Token, on page 28
Configure Transport Settings for Smart Licensing, on page 28
Select License Type, on page 29
Register with Cisco Smart Software Manager, on page 30
Registration, Authorization, and Entitlement Status, on page 32
Out-Of-Compliance and Enforcement Rules, on page 34

Obtain the Product Instance Registration Token

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

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

Procedure

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

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

Step 3 Generate the Product Instance Registration Token.

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

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

Configure Transport Settings for Smart Licensing

Configure the connection mode between Unified CCE and Cisco SSM.

Procedure

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

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

Step 3 Select the connection method to Cisco SSM:

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

  Note Proxy servers that require authentication are not supported for this connection method.

Step 4 Click **Save** to save the settings.

Select License Type

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

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

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

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

Procedure

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

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

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

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

License Type	Licenses
Flex Production	**Unified CCE and Packaged CCE:** • Standard Agent • Premium Agent • Dialer Ports • Server License
Perpetual Production	**Unified CCE and Packaged CCE:** • Premium Agent • Dialer Ports • Server License **ICM:** • Regular Agent • Avaya PG • Third-party IVR licenses • Server License
Perpetual Non-Production	• Regular Agent • Premium Agent • Dialer Ports • Server License • Avaya PG

Step 4 Click **Save**.

Register with Cisco Smart Software Manager

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

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

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

Note You can register your product instance with Cisco SSM or Cisco SSM On-Prem from any ADS server. After the registration, all the AWs show the same registration status.

Procedure

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

Step 2 Click **Register**.

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

Step 3 In the **Smart Software Licensing Product Registration** dialog box, paste the product instance registration token that you generated from Cisco SSM or Cisco SSM On-Prem.

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

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

Table 2: Smart Licensing Status

Smart License Status	Description
On Unsuccessful Registration	
Registration Status	Unregistered
License Authorization Status	Evaluation
Export-Controlled Functionality	Not Allowed
On Successful Registration	
Registration Status	Registered (Date and time of registration)
License Authorization Status	Authorized (Date and time of authorization)
Export-Controlled Functionality	Not Allowed
Smart Account	The name of the smart account
Virtual Account	The name of the virtual account

Smart License Status	Description
Product Instance Name	The name of the product instance
Serial Number	The serial number of the product instance

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

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

Related Topics

Obtain the Product Instance Registration Token, on page 28

Registration, Authorization, and Entitlement Status

Registration Status

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

Table 3: Registration Status

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

Authorization Status

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

Table 4: Authorization Status

Status	Description
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
Authorized	Product is in authorized or in compliance state. Authorization is renewed every 30 days.

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

License Entitlement Status

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

Table 5: License Entitlement Status

Status	Status Description
Authorization Expired	Product authorization has expired, when the product has not communicated with Cisco for 90 days.
Not Authorized	Product instance is not authorized.
Evaluation state	Product is not registered with Cisco.
Evaluation Expired	Product evaluation period has expired.
In Compliance	Product is in authorized or in compliance state. Authorization is renewed every 30 days.
ReservedInCompliance	Entitlement is in compliance with the installed reservation authorization code.
Out-of-Compliance	Product is in out-of-compliance state because of insufficient licenses. It is in an overage period for 90 days before enforcing restrictions.
Not Applicable	Entitlement is not applicable.
Invalid	Error condition state.
Invalid Tag	Entitlement tag is invalid.
No License in Use	Entitlement is not in use.
Waiting	Waiting for an entitlement request's response from Cisco SSM or Cisco SSM On-Prem.
Disabled	Product instance is deactivated or disabled.

Related Topics

Out-Of-Compliance and Enforcement Rules, on page 34

Out-Of-Compliance and Enforcement Rules

Out-of-Compliance

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

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

Enforcement

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

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

  Purchase new licenses to exit the Enforcement state.

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

  Renew the license authorizations to exit the authorization expiry state.

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

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

Note In the Enforcement state, addition of new agents is blocked in Unified CCE.

License States

Smart Licensing has the following states:

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

Note Use **SPOG/CCEAdmin > License Management** to manually renew your registration.

- **Authorization State**
  - **No licenses in use**
  - **Evaluation Mode**—The Product Instance license has an Evaluation period of 90 days. In the Evaluation period you have unlimited access to the product with highest set of product capabilities and unlimited number of licenses. You must register the system with Cisco SSM or Cisco SSM On-Prem within 90 days. If the system is not registered before the end of the evaluation period, it will be moved to the Enforcement state where certain system functions are restricted.
  - **In Compliance**—When the license consumption is as per the purchased quantity, the product is compliant.
  - **Evaluation expired**—Product Instance evaluation period has expired.
  - **Authorized**—Product Instance is in authorized or in compliance state. Authorization is renewed every 30 days.
  - **Out of Compliance**—Product Instance reports license usage to Cisco SSM every 15 minutes. If your license consumption is more than the entitlements for five consecutive reporting intervals, the Product Instance is transitioned to the Out of Compliance state.

    The out-of-compliance period is for 90 days, within which you need to purchase the additional licenses. If you fail to take corrective action within the 90 days period, the Product Instance is transitioned to the Enforcement state.
  - **Authorization Expired**—Product Instance authorization has expired. This usually happens when the product has not communicated with Cisco SSM for more than 90 days. It is in an overage period for 90 days before restrictions are enforced.

Note Use **SPOG/CCEAdmin > License Management** to manually renew your authorization.

- **Enforcement State**

  When the 90 day period of Out-of-Compliance, Evaluation Period or Authorization period has expired, the Product Instance is moved to the Enforcement state in which system operations are impacted for Contact Center components. The Product Instance is in the Enforcement state in the following scenarios:
  - **Out-of-Compliance expiry**—When the out-of-compliance period of 90 days has expired.

    Purchase new licenses to exit the Enforcement state.
  - **Authorization expiry**—When the Product Instance has not communicated with Cisco SSM or Cisco SSM On-Prem for 90 days and has not automatically renewed the entitlement authorizations.

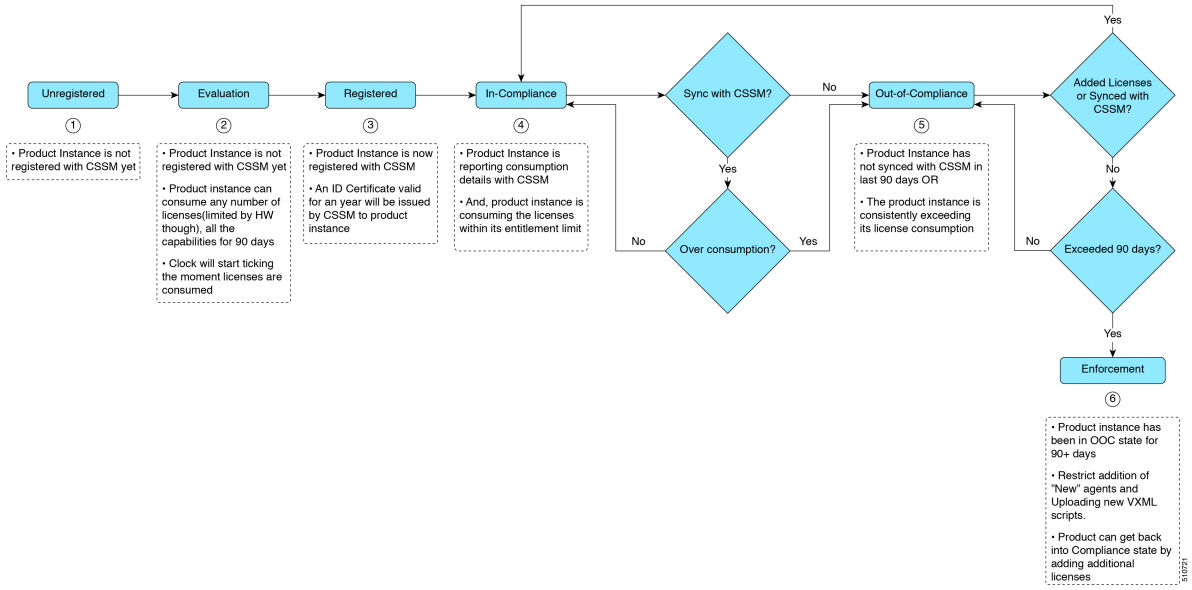
    Renew the license authorizations to exit the Authorization expiry state.

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

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

A pictorial representation of different license states is as follows:

Figure 1: License States



Notifications and Alerts

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

Following are some of the notification methods:

- Banner Notifications
- System Alerts

Banner Notifications

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

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

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

System Alerts

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

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

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

License Consumption Calculation

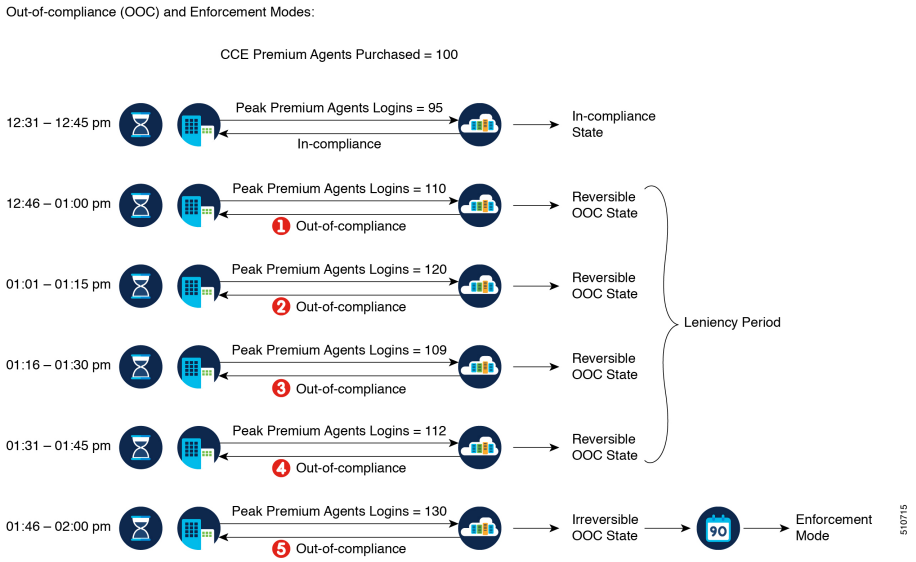
The system reports peak license usage to Cisco SSM every 15 minutes. If in five consecutive reports you are seen to have consumed more licenses than you are authorized to, the Product Instance is pushed to the Out-of-Compliance state. The Out-of-Compliance period is for 90 days, within which you need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

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

License Computation Scenario 1

License purchased: 100 licenses

Figure 2: License Computation



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

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

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

License Computation Scenario 2

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

License Purchased: 100 licenses

Figure 3: License Computation

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

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

New Deployments

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

Migrate to Smart Licensing

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

License Management

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

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

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

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

Related Topics

Configure Transport Settings for Smart Licensing, on page 28

Smart Licensing Tasks

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

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

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

Note You have to Deregister and Reregister manually.

Related Topics

Renew Authorization, on page 40
Renew Registration, on page 41
Reregister License, on page 41
Deregister License, on page 42

Renew Authorization

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

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

Procedure

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

Step 2 Click **Action** > **Renew Authorization**.

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

Renew Registration

Use this procedure to manually renew your certificates.

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

Procedure

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

Step 2 Click **Action** > **Renew Registration**.

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

Reregister License

Use this procedure to reregister Unified CCE with Cisco SSM or Cisco SSM On-Prem.

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

Procedure

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

Step 2 Click **Action** > **Reregister**.

Step 3 In the **Smart Software Licensing Product Registration** dialog box, paste the copied or saved Registration Token Key that you generated using the Cisco SSM or Cisco SSM On-Prem in the Product Instance Registration Token text box.

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

Step 5 Close the window.

Deregister License

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

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

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

Procedure

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

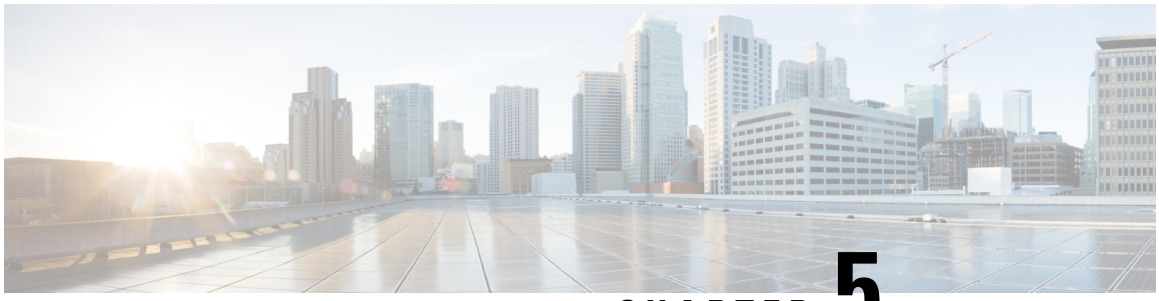
Step 2 Click **Action** > **Deregister**.

Step 3 On the **Confirm Deregistration** dialog box, click **Yes** to deregister.

Best Practices

Some of the best practices for Smart Licensing are:

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



CHAPTER 5

CCEDataProtect Tool

CCEDataProtect Tool

CCEDataProtect Tool is used to encrypt and decrypt sensitive information that the Windows registry stores in it.

Note Only the administrator, domain user with administrator rights, or a local administrator can run the CCE DataProtect Tool, using `<Install Directory>:\icm\bin\CCEDataProtectTool.exe`.

Following are the features supported with the CCEDataProtect Tool:

- **DBLookUp** - view and edit External DBLookUp SQLLogin registry value.

  DBLookUp supports the following options:

  - **Decrypt and View** - to view the encrypted password stored in the SQLLogin registry as clear text.
  - **Edit and Encrypt** - to configure the registry with encrypted value for first time or edit the existing encrypted value stored in the registry.
  - **Help** - information about the DBLookUp options.
  - **Exit** - to return to the initial menu.

- **Rekey** - use this functionality with the Common Ground upgrade to re-encrypt the encrypted values based on upgraded software version. For Technology Refresh upgrade, you must reconfigure the value in the destination machine using the **Edit and Encrypt** option. It is recommended to use the **Rekey** option to secure the sensitive information.

Important **Rekey** option will be supported in the future releases only.

- **Help** - information about the CCEDataProtect Tool options.
- **Exit** - to exit the CCEDataProtect Tool.

Related Topics

Configure External DBLookUp Registry Value using CCEDataProtect Tool, on page 44

Configure External DBLookUp Registry Value using CCEDataProtect Tool

Perform this procedure to configure the External DBLookUp registry value using the CCEDataProtect Tool.

Procedure

Step 1 Run **CCEDataProtect Tool** from **`<Install Directory>:\icm\bin\CCEDataProtectTool.exe`**.

Step 2 In the Main menu, press **1** to select **DBLookUp**, and press **Enter**.

Step 3 Enter a valid Instance Name for which this option is configured.

Note You can run only one instance of CCEDataProtect Tool at a time.

Step 4 Press **2** to select **Edit and Encrypt**, and press **Enter**.

The tool displays the current encrypted value stored in the registry as clear text, if it is already configured.

a) Enter a new Registry Value at the system prompt, and press **Enter**.

Note The maximum limit for the External DBLookUp registry entry is 2048 characters.

If you press **Enter** without entering any value, the system removes the encrypted value stored in the registry. You can use this option to remove the encrypted entry.

b) When the system displays the message: `Are you sure you want to Edit the Registry Details [Y/N]`, press **Y** and then press **Enter**.

The system updates the Registry with an encrypted value and the system prompts the message: `Registry Updated with Encrypted Data Successfully`.

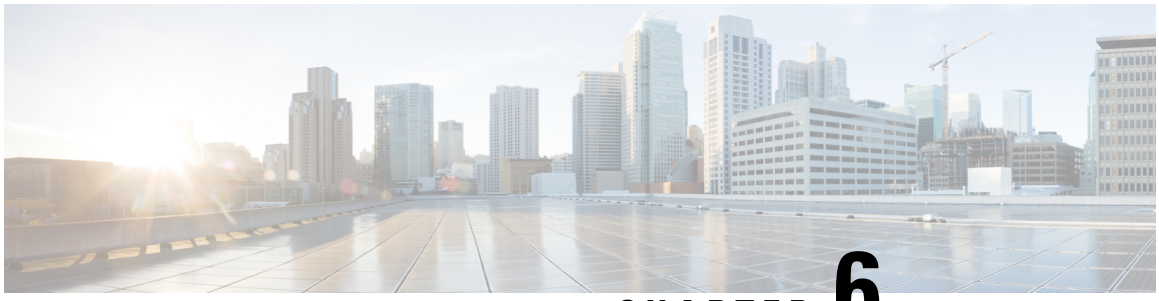
Step 5 Press **1** to select **Decrypt and View**, to verify the encrypted password.

Note CCEDataProtect Tool generates the following logs in the `C:\temp` folder.

- `CCEDataProtectTool.log` - captures the tool usage by the administrator.
- `CCEDataProtectTool_audit.log` - captures the audit details of the tool usage.

Related Topics

CCEDataProtect Tool, on page 43



CHAPTER 6

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

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. • **General** tab: Fields are read-only. • **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

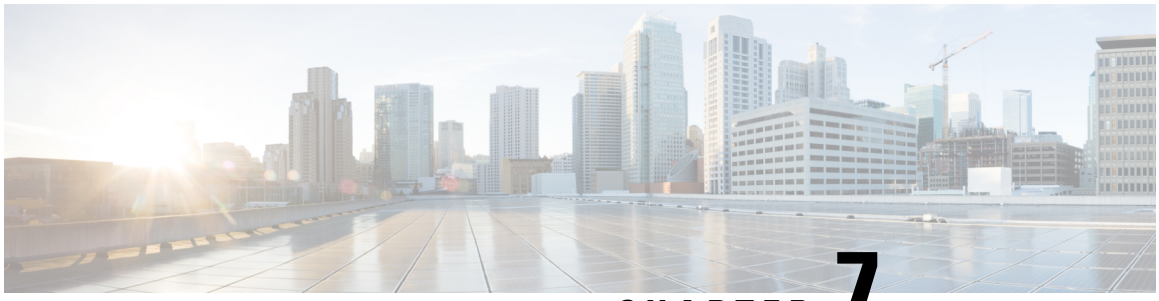
To configure network transfer from an agent desktop, complete the following steps.

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.



CHAPTER 7

Voice Call Routing

Routing a Target Device in Unified CCE

The following procedures outline the steps to follow each time you want to route to a new device target in Unified CCE.

Target Device Routing on Unified CM

Procedure

Step 1 Create a CTI Route Point on the Unified CM.

This step configures the Unified CM to make a route request to the system software when the Route Point is dialed.

Step 2 Associate the CTI Route Point with the PG User.

This step makes the Route Point visible to the system software.

Route Target Device Using Configuration Manager

Procedure

Step 1 Create a new Dialed Number using the Configuration Manager.

Defines a new entry point for call routing.

Step 2 Add a new Call Type using the Configuration Manager.

Allows you to categorize calls and route them appropriately.

Step 3 Associate the Dialed Number with the Unified ICM Call Type.

Allows you to map the Dialed Number to a routing script.

Step 4 Create a new routing script using the Script Editor.

Routes the call to the entry point.

Step 5 Associate the Call Type with the routing script.

Associates the Call Type with the routing script.

Note

- In a Unified Communications Manager cluster, be aware that two routing clients must not share the same CTI Route Point. Each routing client must use distinct CTI Route Points in a Unified Communications Manager cluster.
- Only one unique Dialed Number can be assigned to a CTI Route Point across all partitions. When setting up a new CTI Route Point, avoid using a Dialed Number that is already assigned to a different CTI Route Point in another partition. Using different Dialed Numbers for different partitions for a CTI Route Point is not a supported configuration.
- When you configure a calling party transformation mask for the translation pattern in Unified Communications Manager, the application will have additional connections and disconnections. Therefore, for the components to function properly, do not configure a translation pattern mask for the calling party.

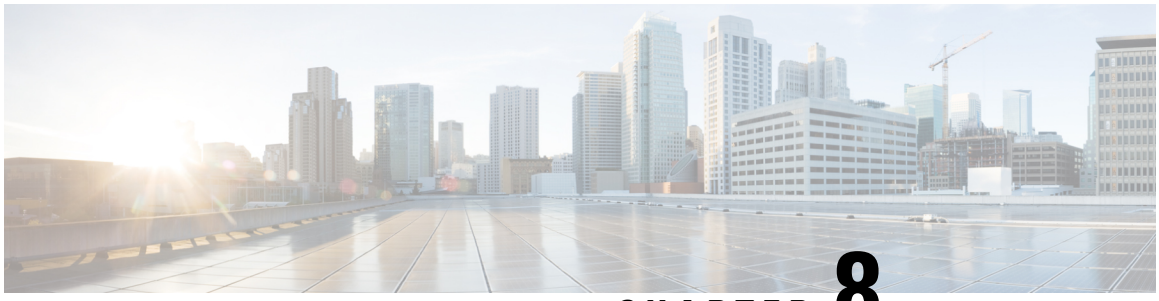
Peripherals and Skill Groups

Only base skill groups are supported for Unified CCE configurations. A default is set at the peripheral level, ensuring that any new skill group created is base-only.

Agents must be associated with skill groups or precision queues. You can create precision queues using the Unified CCE Web Administration.

For more information about creating routing scripts, see *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise* and the Script Editor online help.

For more information about configuring Unified CCE, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide*



CHAPTER 8

Dialed Number Plan

About Dialed Number Plan

The Dialed Number Plan allows you to manage and track agent-initiated calls.

The Dialed Number Plan applies only to calls initiated by the agent on their soft phone and *not* on their hard phone. Calls made on the hard phone are not subject to the permission, interpretation, translation, posting routing, and so on, specified in the Dialed Number Plan.

Dialed Number Plan Explained

The Dialed Number Plan consists of a number of entries intended to accommodate the different types of calls agents might make. Each entry contains a wildcard string that is used to match a number that an agent might dial. Each digit of the string is processed until a matching dial plan entry is found. When found, the selected trunk group or resource is used to complete the call.

Each entry contains additional information indicating how to handle the calls matching that wildcard string.

For example, dialing a 9 to receive an outside line on a PBX or ACD is specified in the dial plan. All patterns that reference network trunks might begin with a “9” digit. Subsequent digits might be “1” for long distance patterns, “0” for operator assisted or international calls, “2” through “9” to specify an area code. The dial plan allows a customer to have multiple phone carrier trunks terminated at the PBX or ACD for different outbound call types. A customer might choose MCI as the long distance carrier while AT&T is the international carrier, and Bell Atlantic is the local carrier. The dial plan configuration is used to determine which carrier to use based on the patterns defined within the dial plan.

Note Do not confuse the Dialed Number Plan Bulk Insert tool with the Dialed Number Bulk Insert tool.

You use the Dialed Number Plan to:

- Ensure agent-initiated calls are routed by a Unified ICM routing script
- Set up basic dialing substitutions

Dialed Number Plan and Routing of Agent Calls

The most common and powerful use of the Dialed Number Plan is to ensure that agent-initiated calls are routed through the system software. In this case, you must specify that you want to request a PostRoute for the call and specify a dialed number associated with a routing script designed to handle the type of agent call.

Use this method of configuring the Dialed Number Plan for:

- Agent-to-agent transfers
- Agent-to-agent calling
- Agent-initiated outbound calls

Dialed Number Plan and Basic Dialing Substitutions

You can also use the Dialed Number Plan to specify basic dialing substitutions. In this scenario, you identify a wildcard pattern to match the number dialed by an agent. However, you do not request a Post Route and the call is *not* matched to a Dialed Number, and thus not routed by the system software. Instead, you enter the string you want to be dialed in the Dial String field. That string is used to place the agent's call.

Using the Dialed Number Plan in this way is most useful for setting up such things as:

- Speed dial
- Using alphanumeric characters to dial from a soft phone

Dialed Number Plan Values

Each field on the **Dialed Number Plan** dialog box is defined in the Configuration Manager online help. This section provides additional information about these fields and how you can use them to set up agent dialing for your contact center.

Wildcard Pattern

The wildcard pattern you enter can contain letters, digits, and number signs (#). It can also include the following wildcard characters.

Character	Description
?	Represents any single alphanumeric character.
!	Represents any string of character and can appear only at the end of a pattern.

Routing Client

The Routing Client field lets you specify the routing client for the agent call. In Unified CCE configurations, set this field to identify the Unified CM PG.

Post Route

Use the Post Route field to specify whether this type of agent call will be sent to a routing script. If you set Post Route to **Yes**, you must also enter a Dialed Number that is associated with a routing script designed to handle the type of agent call.

Dialed Number

Use the Dialed Number field if you have set the Post Route field to **Yes**, indicating that you want a Unified ICM routing script to handle this agent call.

Dial String

Use the Dial String field only when you set the Post Route field to **No**, indicating that you want to use this entry for dialing substitutions. This field cannot be used when PostRoute is selected to send the call to a Unified ICM routing script.

The Dial String field can contain wildcard characters used to translate the dialed number string provided by the agent to the dial string that will be delivered to the switching platform. The following table describes the wildcard characters that might appear in the DialString field.

Wildcard Character	Description
!	Matches any group of characters
?	Matches any single character
X or x	Excludes the character in the agent supplied dialed number string at the position identified from the offset as defined from the beginning of the DialedNumberPlan DialString field

The following table provides examples of the translation of a DialedNumber string specified by an agent to a resultant DialString as defined by the DialString entry of the matching DialedNumberPlan entry.

Agent Dialed Number	DialedNumber Plan Dial String	Dial string result	Description
5133	6100	6100	Direct substitution.
5133	6X???	6133	Partial replacement.
5133	!	5133	Complete Copy.
5133	9275!	92755133	Prefix Addition.
5133	62XX??	6233	First 2 char substitution.
5133	????	5133	Complete Copy.
5133	?XXX000	5000	Retain first character; substitute the remaining characters.
2755100	????200	2755200	Replace last three characters.

Agent Dialed Number	DialedNumber Plan Dial String	Dial string result	Description
2755100	!220	2755100220	Suffix addition.

Dial String Configuration for Speed Dialing

You can configure Static Dial String translations to provide speed dial capabilities. Here, you enter the abbreviated string an agent dials in the wildcard pattern. You enter the actual target number in the Dial String of the entry.

When a dialed number (provided by an agent) matches the wildcard pattern of the Dialed Number Plan entry, the Dial String configured entry is sent in place of the agent supplied Dialed Number string.

The following table provides an example of a speed dial configuration.

Agent Dialed Number	Wildcard Pattern	Dial String	Result
133	1??	919782755!	919782755133

Dial String Configuration for Alphanumeric Substitutions

You can use the Dialed Number Plan to allow agents to specify an alphanumeric string when dialing. For instance, an agent might dial **SALES** when calling the sales department rather than a numeric value that might be harder to remember.

To configure an alphanumeric substitution, configure the alphanumeric dial string as the wildcard pattern and the target number as the Dial String of the DialedNumberPlan entry. When a dialed number provided by an agent matches the wildcard pattern of the Dialed Number Plan entry, the configured Dial String is sent in place of the agent supplied string.

You can combine wildcard characters with this feature to allow Alpha prefixes to be added to numbers to identify the location of the number. Examples are shown the following table.

Agent Dialed Number	DialedNumberPlan Dial String	Resultant Dial String
SALES	919782755100	919782755100
BOS5133	9782755133	9782755133
FL14Office1433	5133	5133

Dial Number Type Plan

The Dial Number Type Plan lets you specify the type of call that will be placed.

Dialed Number Plan	Description
International	Allows agents to place calls classified as international calls.
National	Allows agents to place calls classified as national long distance calls.

Dialed Number Plan	Description
Local	Allows agents to place calls classified as national local calls.
Operator Assisted	Allows agents to place calls classified as operator assisted calls.
PBX	Allows agents to place calls to agents on the same peripheral.

The options for this field map exactly with the options on the agent desk settings list window. The system software checks the agent desk settings for the agent placing the outbound call. agent desk settings define which types of calls agents are permitted to make. If the agent desk settings for an agent prevent them from placing a particular type of call (for instance, international), the call is not placed.

Dialed Number Plan Configuration

Use Dialed Number Plan to Ensure Routing of Agent Calls

Follow these steps to configure a Dialed Number Plan entry to route an agent call through the system software.

Procedure

Step 1 Create a routing script to handle each type of agent-initiated call using the Script Editor.

This step ensures agent-initiated calls are routed appropriately by the system software.

The script can target agent, services, or skill groups using Unified ICM script nodes. When a target is chosen, the associated label is sent back to the requesting peripheral. The label value is substituted for the dial string specified by the agent and sent to the switching platform to place the outbound call.

Step 2 Select **ICM Configuration Manager** > **Tools** > **List Tools** > **Call Type List**.

Allows you to set up the call type and associate it with the dialed number to target to routing scripts.

Note You can also use a pre-existing call type and script.

Step 3 Select **ICM Configuration Manager** > **Tools** > **Bulk Configuration** > **Insert** > **Dialed Number Plan Bulk Insert** and insert an entry in the Dialed Number Plan dialog.

Using the fields in this window, make sure to:

- Indicate the appropriate wildcard character.
- Set the Post Route text box to **Yes**.
- Select a valid Dialed Number associated with the routing script used to route the agent call.
- Set the Dial Number Type Plan to indicate the type of call.

This step matches the agent's dialed string to a Dialed Number. This ensures the agent's call will be routed by a Unified ICM routing script.

Step 4 Select **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Desk Settings List** and ensure that Agent Desk Settings are set to identify the types of calls agents can place.

Ensures that agents are allowed to or restricted from placing different types of outbound calls.

Use Dialed Number Plan to Set Up Basic Dialing Substitutions

Follow these steps to configure a Dialed Number Plan entry to do basic dialing substitutions:

Procedure

Step 1 Insert an entry in the Dialed Number Plan dialog box by selecting **ICM Configuration Manager** > **Tools** > **Bulk Configuration** > **Insert** > **Dialed Number Plan Bulk Insert**.

Using the fields in this window, make sure to:

- Indicate the appropriate wildcard character.
- Set the PostRoute field to **No**.
- Identify a valid Dial String used to place the call.
- Set the Dial Number Type Plan to indicate the type of call.

Matches the agent's dialed string to the Dial String indicated in the entry. This Dial String is used to place the call (the call will not be routed by the system software).

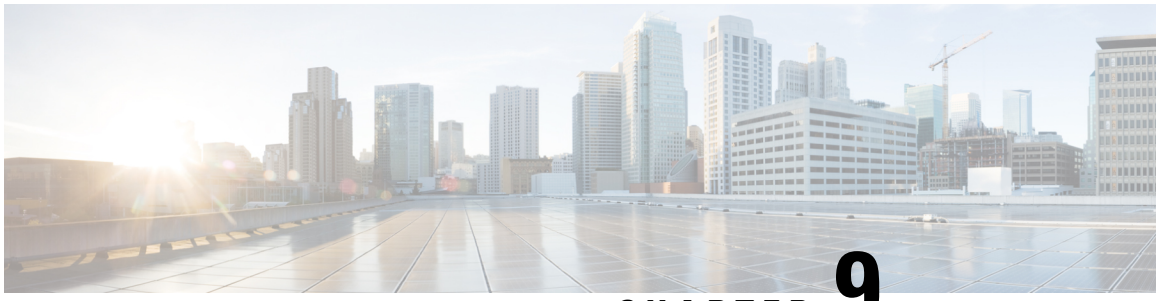
Step 2 Ensure agent desk settings are set to identify the types of calls agents can place by selecting **ICM Configuration Manager** > **Tools** > **List Tools** > **Agent Desk Settings List**.

Ensures that agents make only the types of outbound calls they are permitted to make.

For more information about Unified ICM Routing Scripts, see *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise*

Related Topics

Agent Desk Settings Configuration, on page 3



CHAPTER 9

Web Based CCE Administration

Unified CCE Web Administration

The Configuration Manager enables you to perform most of the Unified CCE administrative tasks. The gadgets in the Unified CCE Web Administration application enables you to manage other Unified CCE administrative tasks and system settings.

Note

- For more information on each gadget, please see the online help available in the **CCE Web Administration** page.
- Users are logged out of the Unified CCE Administration console automatically after 30 minutes of inactivity.

Access Unified CCE Administrative Gadgets

To manage agents, attributes, precision queues, bucket intervals, media routing domains, license, and bulk jobs, use the corresponding card in the Unified CCE Web Administration application. For example, to access business hours:

Procedure

Step 1 From your desktop, double-click the **Unified CCE Tools** icon, and then select **Administration Tools**.

Step 2 Double-click the **CCE Web Administration** link.

Step 3 From the left navigation bar, select **Overview** and then select **Organization Setup** card.

Step 4 Select **Business Hours**.

Note For more information about business hours, see Business Hours.

Access Unified CCE System Management Gadgets

To configure system settings such as deployment type and system information, use the **Infrastructure Settings** card. To configure Single Sign-On (SSO), use the **Features** card in the Unified CCE Web Administration application. For example, to set the deployment type:

Procedure

Step 1 From your desktop, double-click the **Unified CCE Tools** icon, and then select **Administration Tools**.

Step 2 Double-click the **CCE Web Administration** link.

Step 3 Select **Deployment Settings**.

Step 4 On the **Deployment Type** page, click on deployment type and then select an instance from the drop-down list.

Note For more information about deployment type, see Deployment Type.

Managing Agents

The Agents tool in Unified CCE Administration contains a list of agents. These agents are created in **Agent Explorer** under **Configuration Manager**.

Rows in the list show the following fields for each agent:

- Username
- Peripheral
- Last Name
- First Name
- Description

The username maps to the login name in **Agent Explorer**.

You can search and sort this list, and you can click the row for an agent to open the **Edit Agent** window. You can only edit an agent's attribute settings.

You cannot create or delete agents in this tool. You must create or delete agents in the **Configuration Manager Agent Explorer** tool.

Note Ensure that Agent ID (Peripheral number) and agent Login name is unique for each user.

Related Topics

Agent Reskilling, on page 11

Attributes

Attributes identify a call routing requirement, such as language, location, or agent expertise.

You can create two types of attributes:

- Boolean
- Proficiency

Use Boolean attributes to identify an agent attribute value as **true** or **false**.

For example, you can create a **Boston** attribute. This attribute specifies that the agent assigned to this attribute must be located in Boston. An agent in Boston would have Boston as *True* as the term for that attribute.

Use Proficiency attributes to establish a level of expertise in a range from *1 to 10* , with 10 being the highest level of expertise.

For example, for a Spanish language attribute, an original speaker would have the attribute Proficiency as *10*. When you create a precision queue, you identify which attributes are part of that queue and then implement the queue in a script.

When you assign a new attribute to an agent and the attribute value matches the precision queue criteria, the agent is automatically associated with the precision queue.

Note Attributes is a prerequisite for Precision Queue.

Precision Queues

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

Related Topics

Precision Queues, on page 79

Managing Bucket Intervals

Configure bucket intervals to report on how many calls are handled or abandoned during specific, incremental time slots.

Each bucket interval has a maximum of nine configurable time slots, called Upper Bounds. Upper Bounds are ranges measured in seconds to segment and capture call-handling activity. You can run reports that show calls answered and calls abandoned for these intervals.

If your goal is to have calls handled within 1 minute, you might set up **Upper Bounds** for intervals that show how many calls are handled in less than or more than 1 minute. Intervals might be for 30, 60, 80,120, 150, 180, and 240 seconds. Using these intervals, you can see if calls are being answered within 1 minute or if callers are waiting longer.

The intervals also give you insight into how long callers are willing to wait before cancelling a call. Perhaps many callers do not abandon a call until they have waited for two minutes. This might indicate that you can modify your goal.

You can associate bucket intervals with call types, skill groups, and precision queues. The system automatically creates a built-in bucket interval, which you cannot edit or delete.

Related Topics

Precision Queues, on page 79

Media Routing Domains

Media Routing Domains (MRDs) organize how requests for each communication medium, such as voice and email, are routed to agents.

An agent can handle requests from multiple MRDs.

For example, an agent can belong to a skill group in an MRD for email and to a skill group in an MRD for voice calls. Configure at least one MRD for each communication medium your system supports. You do not need to configure an MRD for voice; the Cisco_Voice MRD is built in. You can add and update only Multichannel MRDs using the Unified CCE Administration Media Routing Domain tool.

Note To add or update Multichannel MRDs for Enterprise Chat and Email, use the Configuration Manager Media Routing Domain List tool.

Manage Bulk Jobs

Bulk jobs are a fast and efficient way to migrate existing agent and supervisor to single sign-on accounts.

Note Do not run bulk jobs during heavy call load.

Note Supervisors have no access to the Bulk Jobs tool.

Deployment Type

The deployment type you select, significantly impacts the call processing capacity, configuration limits, smart license type, and access to the features and configuration tools. The configuration steps vary for every deployment type.

You can select any one of the following deployment types:

- Packaged CCE Deployment types:
  - Packaged CCE: Lab Mode
  - Packaged CCE:2000 Agents
  - Packaged CCE: 4000 Agents
  - Packaged CCE: 12000 Agents
- HCS for Contact Center deployment types:
  - HCS-CC: 2000 Agents
  - HCS-CC: 4000 Agents
  - HCS-CC: 12000 Agents
  - HCS-CC: 24000 Agents
- Unified CCE deployment types:
  - UCCE: Progger (Lab Only)
  - ICM Rogger (Non-Reference Design)
  - ICM Router/Logger (Non-Reference Design)
  - UCCE: 8000 Agents Router/Logger (Non-Reference Design)
  - UCCE: 2000 Agents
  - UCCE: 4000 Agents Rogger
  - UCCE: 12000 Agents Router/Logger
  - UCCE: 24000 Agents Router/Logger
  - Contact Director

Note For information on using the gadget after you select a deployment type, see the *Cisco Unified Contact Center Enterprise Developer Reference Guide* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-programming-reference-guides-list.html and the online help.

Settings

The system can support a defined call capacity based on deployment model. Exceeding the supported rate of incoming calls degrades performance and can result in late calls, dropped calls, delivery of new incoming calls, the time out of requests, and potential system failures. (Call transfers are permitted.)

The System Information tool enforces limits to protect against overloading the system and establishes continuous monitoring of the incoming call rate according to the configured settings.

Single Sign-On (SSO)

The Single sign-on (SSO) is an authentication and authorization process. Authentication proves you are the user you say that you are, and authorization verifies that you are allowed to do what you are trying to do.

SSO allows users to sign in to one application and then securely access other authorized applications without a prompt to provide the user credentials once again. SSO permits Cisco supervisors or agents to sign on only once with a username and password to gain access to all of their Cisco browser-based applications and services within a single browser instance.

By using SSO, Cisco administrators can manage all users from a common user directory and enforce password policies for all users consistently.

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

Business Hours

Business hours are the working hours during which you conduct business. You can create and modify business hours and set weekly and daily schedules for each business hour. You can create different business hour schedules for regular working days and holidays. You can also open or close the business hours if there is an emergency.

You can define the status reasons for business hours and assign codes for each status reason. Status reason is required when you force open or force close a business hour, and when you add special hours and holidays.

Add and Maintain Business Hours

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours**.

Step 2 On the **Business Hours** page, click **New** to open the **New Business Hours** page.

Step 3 Complete the following information on the **General** tab and click **Save**.

Field	Required?	Description
Status	-	Select one of the following statuses for the business hour: • **Open/Closed as per Business Calendar** • **Force Open** • **Force Close**
Status Reason	Yes, if the status is Force Open or Force Close.	This field is enabled only if the status is Force Open or Force Close. Search and select a status reason for the business hour.
Name	Yes	Enter a unique name for the business hour. Maximum length is 32 characters. Valid characters are alphanumeric, period (.), and underscore (_). The first character must be alphanumeric.
Description	No	Enter a description of the business hour.
Time Zone	Yes	Select a time zone of the business hour from the drop-down list.
Department	-	Search and select a department to associate with the business hour. Default is Global. **Note** This is applicable for Packaged CCE deployment only.

Step 4 Click the **Regular Hours** tab and complete the following information:

- Select one of the following **Business Hour Type**:
  - **24x7**: Always open. You cannot customize the working hours.
  - **Custom**: You can customize the working hours.
- If you select **Custom**, enable at least one business day and select the **Start Time** and **End Time**.

Step 5 Click the **Special Hours & Holiday** tab. You can either add or import special hours and holidays.

Step 6 Click **Add** to open the **Add Special Hours & Holiday** popup window. Complete the following information:

Field	Required?	Description
Date	Yes	Select a date from the calendar.
Description	No	Enter a description for the special hour.
Status	-	Select a status. If the status is **Open**, the **Start Time** and **End Time** fields are enabled.

Field	Required?	Description
Start Time	Yes, if status is Open.	Select a start time for the special hour.
End Time	Yes, if status is Open.	Select an end time for the special hour.
Duration	-	Displays the duration of the special hour.
Status Reason	Yes	Search and select a status reason.

Step 7 Click **Save** to add the special hours and holidays.

Step 8 To import special hours and holidays, follow these steps.

a) Click **Import** to open the **Import Special Hours and Holidays** pop-up window.

b) Click the download icon to download the Special Hours & Holidays template. Use this template to enter the special hours and holidays.

c) Click **Choose File** and browse to the special hours and holidays file. Click**Import** to upload the file.

Note The file must contain at least one special hour and holiday.

The file must be in CSV format with a file extension as .txt or .csv.

Step 9 Click **Export** to download the special hours and holidays in .csv format.

Step 10 Click **Save**.

Note The imported business hours overwrites the existing ones.

Add Business Hours by Copying an Existing Business Hour Record

You can create a new Business Hour record by copying an existing Business Hour record.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours**.

Step 2 Click the Business Hour you want to copy, and then click the **Copy** button in the Edit <Business Hour> page. The **New Business Hour** page opens.

Step 3 Enter **Name** and **Description** for the Business Hour.

Step 4 Review the rest of the fields on the **General**, **Regular Hours**, and **Special Hours & Holiday** tabs that were copied from the original Business Hour record, and make any necessary changes.

Step 5 Click **Save** to return to the List window.

Add Status Reasons

This procedure explains how to add and maintain status reasons for business hours.

Procedure

Step 1 In **Unified CCE Administration**, choose **Organization** > **Business Hours** > **Status Reasons**.

Step 2 Click **Add** to open the **Add Status Reason** popup window.

Step 3 Enter the Status Reason. Maximum length is 255 characters.

Step 4 Enter a unique Reason Code. Range is 1001 to 65535. Codes 1 to 1000 are reserved as system-defined reason codes.

Step 5 Click **Save**.

To add more status reasons, repeat steps from 2 to 5.

Step 6 Click **Done** to return to the List window.

Edit Status for Multiple Business Hours

Perform the following steps to edit the status of multiple business hours at once.

Procedure

Step 1 On the **Business Hours** page, select two or more business hours to edit.

Step 2 Choose **Edit** > **Status** to open the **Edit Business Hours** page.

Step 3 Check the **Status** check box and select the required status.

Step 4 If you select the status as **Force Open** or **Force Close**, search and select a **Status Reason**.

Step 5 Click **Save**.

Edit Schedule for Multiple Business Hours

Perform the following steps to edit schedules of multiple business hours at once.

Procedure

Step 1 On the **Business Hours** page, select two or more business hours to edit.

Step 2 Choose **Edit** > **Schedule** to open the **Edit Business Hours** page.

Step 3 Check the **Time Zone** check box and the select the required time zone from the drop-down list.

Step 4 Check the **Type** check box and select the required business hour type.

Step 5 If you select **Custom**, enable atleast one business day and select the **Start Time** and **End Time**.

Step 6 Click **Save**.

Configure Yearly Schedules

You can configure and maintain Business Hour schedules for the whole year.

Procedure

Step 1 Configure the regular working hours for weekdays.

Step 2 Configure **Special Hours & Holidays** schedules for whole year by doing the following:

a) Add the **Special Hours & Holidays** details for all the special hours and holidays for the whole year into the CSV template file.

b) On the **Import Special Hours & Holidays** page, click **Choose File** and browse to the special hours and holidays file.

c) Click**Import** to upload the file.

After you import the configuration file, the BH configurations are loaded on the Business Hours page. Validate the configurations.

d) Click **Save**.

Note When you update the configured Business Hours, remove any elapsed schedules and then update the new schedules for any new special hours or holidays in a Business Hour configuration.

Cloud Connect Administration

Cloud Connect is a component that hosts services that allow customers to use cloud capabilities such as Cisco Webex Experience Management and CCE Orchestration.

The administrator should configure the Cloud Connect server settings in the Finesse Administration console to contact the Cisco cloud services. For more information, see *Cloud Connect Server Settings* section in Cisco Finesse Administration Guide at https://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-maintenance-guides-list.html

Initial Configuration for Cloud Connect

Before adding Cloud Connect to the inventory, you will have to install the certificates from both Cloud Connect publisher and subcriber.

For more information, see the section *Certificates for CCE Web Administration* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Procedure

Step 1 In the Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings**, click **Inventory**.

Step 2 In the Inventory page, click **New** to add the new machine to the System Inventory.

Step 3 In the Add Machine dialog box:

a) Select **Cloud Connect Publisher** from the Type list.
b) Enter Hostname or IP Address of the Cloud Connect Publisher Node.
c) Enter Username and Password for your Cloud Connect cluster Administrator.
d) Click **Save**.

Note When you configure Cloud Connect Publisher, its Cloud Connect Subscriber is added to the Inventory automatically.

Edit Cloud Connect Configuration

Procedure

Step 1 In the Unified CCE Administration, navigate to **Overview** > **Infrastructure Settings**, click **Inventory**.

Step 2 Click the Cloud Connector Publisher device to open the Edit window.

Note If you edit the Cloud Connect Publisher, the Cloud Connect Subscriber associated with the publisher is updated automatically. You cannot edit Cloud Connect Subscriber from the Inventory page.

Step 3 Edit the Username and Password for your Cloud Connect cluster Administrator.

Step 4 Click **Save**.

Monitor Server Status Rules

In CCE deployments, the Unified CCE Administration page displays the total number of alerts for machines with validation rules. Click the alert count to view the list of all alerts for each machine. Upon clicking Alerts for the respective machine, you can view the details of the alerts grouped by the following categories:

Server Status Category	Description	Example Rules
Configuration	Rules for installation and configuration of a component. These rules identify problems with mismatched configuration between components, missing services, and incorrectly configured services.	**Cloud Connect:** The status and alerts will appear only if the Cloud Connect is added to the Inventory. **Note** When the machine status is out of sync, every 10mins auto sync will be triggered to synchronize the machine configuration.
Operation	Rules for the runtime status of a component. These rules identify services and processes that cannot be reached, are not running, or are not in the expected state.	

Delete Cloud Connect Configuration

Procedure

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

Step 2 Hover over the Cloud Connect Publisher device and click the **x** icon.

Step 3 Click **Yes** to confirm the deletion.

Note If you delete the Cloud Connect Publisher, the Cloud Connect Subscriber associated with the publisher is deleted automatically. You cannot delete Cloud Connect Subscriber from the Inventory page.

Delete Cloud Connect Subscriber

This section describes how to delete the Cloud Connect subscriber configuration. You cannot delete the publisher node; but you can delete the subscriber node.

Procedure

Step 1 Run the **unset cloudconnect subscriber** command.

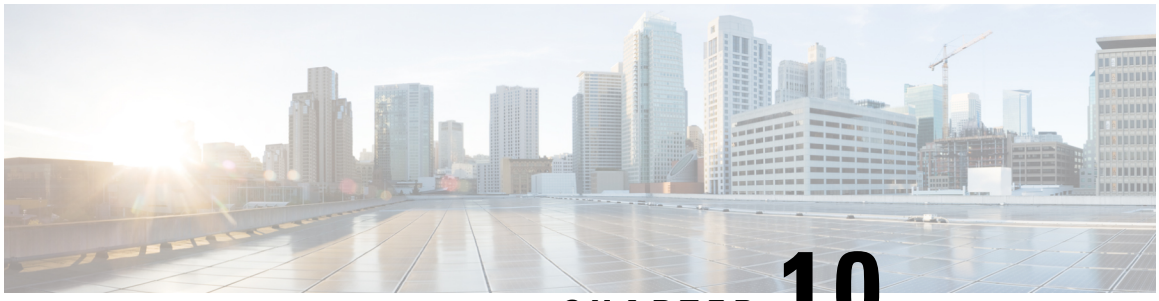
The command removes the Cloud Connect subscriber node configuration from the cluster. For more information, see *Cloud Connect CLI Command* in the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html

Step 2 Power off the subscriber node.

Note When a subscriber node is removed from a cluster, its certificates still exist in the publisher node. The administrator must manually remove the following:

- The certificate of the subscriber node from the trust-store of the publisher node.
- The certificates of the publisher from the trust-store of the removed subscriber node.

Step 3 Run the **utils system restart** command to restart the publisher node.



CHAPTER 10

Precision Queues

Precision Queue Routing

You can create multidimensional precision queues based on predefined business criteria. Agents automatically become members of these precision queues based on their attributes, dramatically simplifying configuration and scripting.

To implement Precision Routing, you create precision queues and implement in your call routing scripts.

A precision queue includes:

- Terms - A term compares an attribute against a value. For example, you can create the following term: English > 6
- Expressions - An expression is a collection of at least one or more terms. For example, if you require an agent who can speak English, is from Dallas and is proficient in sales, you can create the following expression: English > 6 AND Dallas == TRUE AND Sales > 6. You can create up to ten terms for each expression.
- Steps - A step is a collection of at least one or more expressions. When you create a precision queue, you must configure at least one step. You can configure up to ten steps. A step may also include wait time and a Consider If formula. Use wait time to assign a maximum amount of time for the system to wait for an available agent on a step. Use a Consider If formula to evaluate the step at runtime, for example, if the Caller is a Gold or Bronze level.

To configure Precision Routing, you must complete the following tasks:

1. Create attributes.
2. Assign attributes to agents.
3. Create precision queues.
4. Create routing scripts.

Scripting Precision Queues

To implement Precision Routing in your contact center, you must create scripts.

You can create and use configured (static) and dynamic precision queue nodes in your scripts. Static precision queue nodes target a single, configured precision queue. When the script utilizes a single precision queue, use static precision queues. Dynamic precision queue nodes are used to target one or more previously configured precision queues. Use dynamic precision queues when you want a single routing script for multiple precision queues (for example, when the overall call treatment does not vary from one precision queue to another). Dynamic precision queues can simplify and reduce the overall number of routing scripts in the system.

Precision Queues are peripheral gateway (PG) agnostic. Precision queues do not care on which PG an agent resides.

Precision Queue Script Node

You can use the Precision Queue script node to queue a call or task based on caller requirements until agents with desired proficiency become available. This node contains multiple agent selection criterion which are separated into steps.

Figure 4: Precision Queue Script Node

A single call can be queued on multiple precision queues. If an agent becomes available in one of the precision queues, the call is routed to that resource. You cannot reference multiple precision queues with a single Precision Queue node. However, you can run multiple Precision Queue nodes sequentially to achieve this.

The Precision Queue node includes a **Priority** field, which sets the initial queuing priority for the calls processed through this node versus other calls queued to the other targets using different nodes. The priority is expressed as an integer from 1 (top priority) to 20 (least priority). The default value is 5.

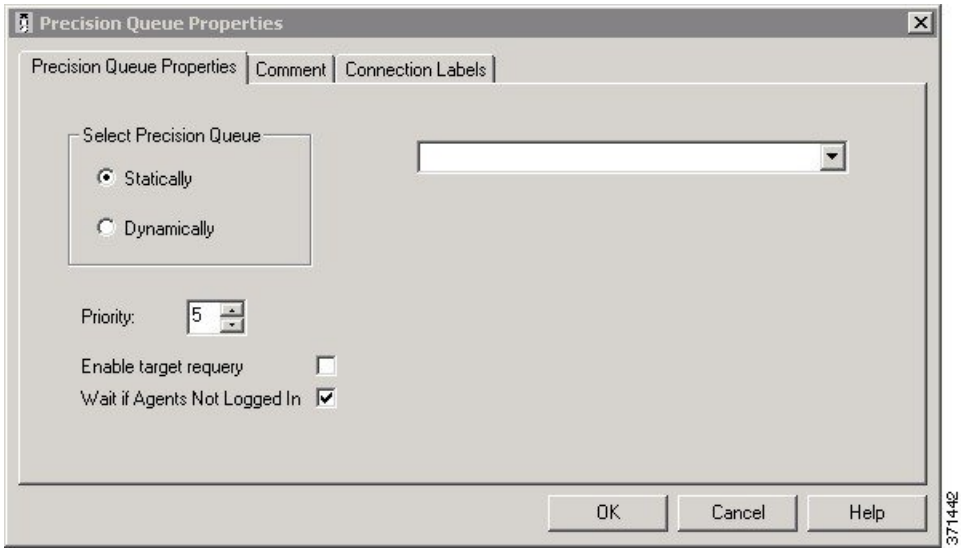
If more than one call is queued to a precision queue when an agent becomes available, the queued call with the lowest priority number is routed to the target first. For example, assume an agent in a precision queue becomes available and two calls are queued to that precision queue. If one call has priority 3 and the other has priority 5, the call with priority 3, the lower value, is routed to the precision queue while the other call continues to wait. If the priorities of the two calls are same, then the call queued first is routed first.

VRU script instructions are not sent to the VRU. If a call enters the Precision Queue node and no resource is available, the call is queued to the precision queue and the node transfers the call to the default VRU, if the call is not already on a VRU. The script flow then exits immediately through the success branch and continues to a Run External Script node to instruct the VRU what to do while holding the call until an agent becomes available. Typically, this invokes a Network VRU script that plays music-on-hold, possibly interrupted on a regular basis with an announcement. The script flow can also use other queuing nodes to queue the same call to other targets, for example, Queue to Skill Group and Queue to Agent.

Precision Queue Properties Dialog Box - Static Precision Queue

The following list describes the **Precision Queue Properties** dialog box for a static precision queue script node.

Figure 5: Precision Queue Properties Dialog Box—Static Precision Queue



The following property is unique to static precision queues:

- **Drop-down list**—To route calls that enter this node to a static precision queue, you must select a precision queue from the list.

The following properties are common to static and dynamic precision queues:

- **Select Precision Queue** radio buttons—You can select one of the following options for each a precision queue:
  - **Statically**—Select this option to choose a single precision queue to be selected for all the calls that enter this node.
  - **Dynamically**—Select this option to select a precision queue on a call-by-call basis based on a formula.

Note Dynamic Precision Queue selection is not available when an External Authorization server is used with Internet Script Editor and will be grayed out in the interface.

- **Priority selection**—To select the initial queuing priority for calls processed through this node, you can select from 1 to 20. The default is 5.
- **Enable target requery check box**—To enable the requery feature for calls processed through this node, select this check box. When a requery occurs, for example if a call is presented to an available agent and the agent does not answer, the script continues through the failure terminal. The script can then inspect the call variable RequeryStatus to determine what to do next. The typical action in case of a No Answer is to queue the call again to other precision queues, and increase the priority so that it is taken out of the queue before regular queued calls.
- **Wait if Agents Not Logged In check box** — When this check box is selected and the agents who are associated with a step are not logged in, then the router will wait for the time that is configured for that

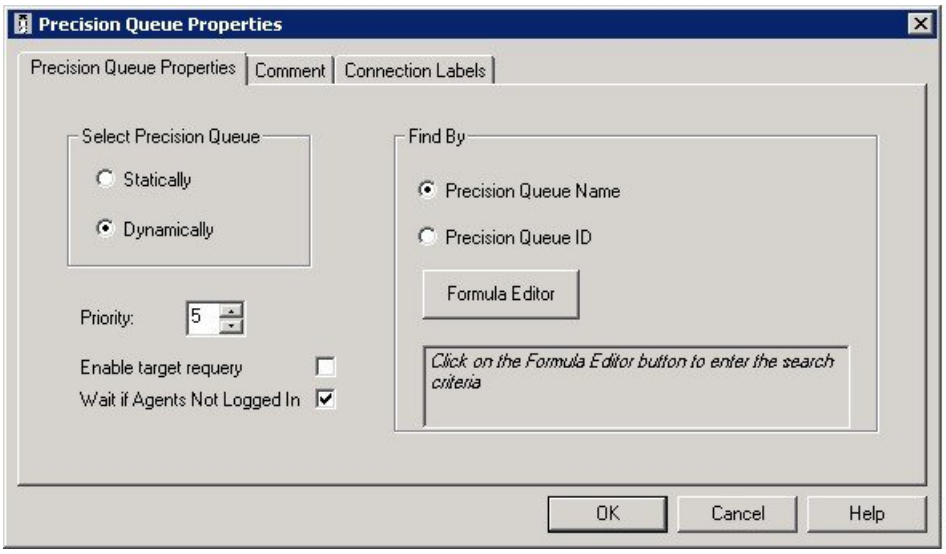
step. When this check box is not selected, the router will not wait on any step. However, on the last step, the router will wait indefinitely irrespective of the selection.

Precision Queue Properties Dialog Box - Dynamic Precision Queue

The following list describes the Precision Queue Properties dialog box for a dynamic precision queue script node.

Use dynamic precision queues when you want a single routing script for multiple precision queues (for example, when the overall call treatment does not vary from one precision queue to another). Dynamic precision queues can simplify and reduce the overall number of routing scripts in the system.

Figure 6: Precision Queue Properties Dialog Box—Dynamic Precision Queue



Note Dynamic Precision Queue selection is not available when an External Authorization server is used with Internet Script Editor and will be grayed out in the interface.

The following properties are unique to dynamic precision queues:

- **Find By radio buttons**—To dynamically route calls that enter this node to a Precision Queue name or ID, use the Find By radio buttons.
  - **Precision Queue Name radio**—Select this option to dynamically route calls that enter this node to a Precision Queue name.
  - **Precision Queue ID**—Select this option to dynamically route calls that enter this node to a Precision Queue ID.
- **Formula Editor button**—To determine to which Precision Queue name or ID to route calls that enter this node, click the Formula Editor button to create a formula. The formula is then evaluated at run time to select a precision queue by either name or by database ID. For example, you can use the formula "Call.PeripheralVariable4" to look up the Precision Queue if call variable 4 contained the Precision Queue name, as a result of a database lookup or from VRU call processing.

Note The section on static precision queues describes the properties that are common to static and dynamic precision queues.

Related Topics

Precision Queue Properties Dialog Box - Static Precision Queue, on page 80

Queuing Behavior of the Precision Queue Node

Precision queues internally are configured with one or more time-based steps, each with a configured wait time. After a call is queued, the first step begins and the timer starts. This occurs although the path of the script exited the success node and a new node may be targeted (for example, Run Ext. Script).

If the timer for the first step expires, control moves to the second step (assuming one exists), and so on. As long as the call remains in queue and there are steps left to perform, the call internally continues to move between steps regardless of the path the call takes after it leaves the precision queue node. If a call is queued to two or more precision queues, the call internally walks through the steps for each precision queue in parallel. After the call reaches the last step on a precision queue, it remains queued on that step until the call is routed, abandoned, or ended.

If there is an update to the precision queue definition, then all queued calls in the precision queue are re-evaluated and are re-run from the first step.

For example, consider the wait time for an ongoing call at step 1 to be 1080 seconds, of which 1000 seconds has already elapsed. Now, suppose the wait time is changed to 900 seconds, then the wait time for this call is also reset to 900 seconds, even though only 80 more seconds are left to move to the next step.

Precision Queue Reports

Reporting provides a complete view of all the queues in the system with both real time and historical metrics. You can use filtering to narrow down the view to specific attributes.

To run real-time or historical reports, you can use Cisco Unified Intelligence Center reporting templates. For more information about Cisco Unified Intelligence Center template reports, see the *Report Template Reference Guide for Cisco Unified Intelligence Center* at http://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-user-guide-list.html.

These reporting templates work with **Precision Routing**:

Agent Real Time - This report displays, for each agent, the active skill group or active precision queue, the state, and the call direction within each media routing domain into which the agent is logged.

Agent Team Real Time - This report displays the current status for each selected agent team and displays the current state and the active skill group or active precision queue for each agent in the selected agent teams.

Call Type Queue Historical All Fields - This report displays the summary statistics for skill groups and precision queues within Call Type ID.

Agent Precision Queue Membership - This report displays selected agents, the media routing domain into which the agent is logged, and the active precision queue with up to the maximum supported number of associated attributes.

Precision Queue Real Time All Fields - This report displays the current status of selected precision queues.

Agent Precision Queue Historical All Fields - This report displays activity for selected agents for a selected interval, sorted by precision queue.

Precision Queue Configuration

Precision queues are a combination of steps that include attributes, defined terms for the selected attributes, wait times, and Consider If formulas.

Precision queues are configured using the **CCEAdmin** > **Organization Setup** > **Skills** > **Precision Queue**

For more information on precision queues and precision routing, see the *Cisco Unified Contact Center Enterprise Features Guide* at http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_feature_guides_list.html.

Configure Precision Queues

Precision Queues are configured using the Precision Queue tool in Unified CCE Administration, not the Configuration Manager.

Before you begin

Before you create precision queues, ensure that you complete the following prerequisites:

- Create attributes.
- Assign attributes to agents.

Procedure

Step 1 In Unified CCE Administration, navigate to **Overview > Organization > Skills > Precision Queue**.

Step 2 Click the **New** button. The page refreshes and a new page appears.

Step 3 In the **Name** dialog box, type a name for the precision queue.

Note You can enter a combination of up to 32 alphanumeric characters and underscores. Precision queue names are case-sensitive.

Step 4 (Optional) In the **Description** dialog box, type any useful information about the precision queue that you wish to note. You can use the description to note the logic behind your queue criteria or for which call type(s) this queue is designed.

Note You can enter a combination of alphanumeric characters and underscores only.

Step 5 Select the **Media Routing Domain** for this precision queue. The field defaults to **Cisco_Voice**. To select a Media Routing Domain: Click the magnifying glass to display the **Select Media Routing Domain** list. Click the link to select a Media Routing Domain and close the list. Click the **X** icon to clear the selection and reapply **Cisco_Voice**.

Step 6 From the **Service Level Type** list, select the service level type to use for reporting on your service level agreement. The default value is **Ignore Abandoned Calls**. In the **Service Level Threshold** dialog box, type the time in seconds that calls are to be answered based on your service level agreement.

Note The time entered in this box is used to report on service level agreements and does not impact how long a call remains in a precision queue. The length of time a call remains in a step is determined by each individual step wait time.

Step 7 From the **Agent Order** list, select one of the following options to determine which agents receive calls from this queue:

- Longest Available Agent - This represents an agent that has been available the longest.
- Most Skilled Agent - This represents an agent that best matches the terms in a step. This is accomplished by totaling the agent's proficiency attribute ratings for that step and selecting the agent with the highest value.
- Least Skilled Agent - This represents an agent that least matches the terms in a step. This is accomplished by totaling the agent's proficiency attribute ratings for that step and selecting the agent with the lowest value.

The default value is **Longest Available Agent**.

Step 8 (Optional) Bucket Intervals. Select the **Bucket Interval** whose bounds are to be used to measure the time slot in which calls are answered. The field defaults to **Use System Default**. To select a different bucket interval: Click the magnifying glass to display the **Select Bucket Interval** list. Click the link to select a bucket interval and close the list. Click the **X** icon to clear the selection and reapply **Use System Default**.

Step 9 Click the numbered step builder link ('Step 1', 'Step 2', and so on). The Step Builder interface pops up. You must build at least one step before you can save the precision queue. Click the magnifying glass in the **Select Attribute** dialog box and select an attribute. The **Select Attribute** dialog box will open with the list of Attributes on the system. You can sort and search through the Attributes. Click on an Attribute name to select it for that term. Click the **X** icon to clear your selection.

Step 10 If you selected a Boolean attribute, from the value list select == (is equal to) or **!=** (does not equal).

OR

If you selected a proficiency attribute, from the operator list, select one of the following operators:

- == (is equal to)
- **!=** (does not equal)
- < (is less than)
- <= (is less than or equal to)
- > (is greater than)
- >= (is greater than or equal to)

Then, for either attribute type, select a value from the values list.

Step 11 To add an additional term, click **Add Attribute** and return to step 7.

OR

To add an additional expression, click the drop down arrow and click **Add Expression** and return to step 7.

OR

Proceed to the next step.

Note When you add an attribute, you can select **OR** or **AND** to specify the logic between the previous and current attributes. The default value is **AND**.

When you add an expression, you can select **OR** or **AND** to specify the logic between the previous and current expressions. The default value is **OR**.

You can add up to 10 expressions or up to 10 terms to a step.

After you add 10 expressions or 10 terms to a step, the **Add Attribute** button is disabled.

To delete a term, click the **X** icon.

If you are not on the last step of the Precision Queue, then you can enter a Wait Time (in seconds). A call will queue at a particular step looking for an available agent matching the step criteria up until the time specified in the wait time field for that step. A blank (or zero) wait time indicates that the call will immediately proceed to the next step if there are no available agents matching the step criteria.

If you are not on the last step of the Precision Queue, then you can enter a Consider If formula for that step.

Consider If expression

You can use a Consider If expression to evaluate a call (within a step) against additional criteria. Each time a call reaches a step with a Consider If expression, the expression is evaluated. If the value for the expression returns as true, the call is considered for the step. If the value returns as false, the call moves to the next step. If no expression is provided for a step, the step is always considered for calls.

Note You cannot add a Consider If expression to the last step.

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

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

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

- Call
- PQ
- Skillgroup
- ECC
- PQ Step
- Call Type
- You can use custom functions in a Consider If expression and you can create custom functions (in Script Editor).

Example:

Consider If expression examples

PQ.PQ1.LoggedOn > 1 - Evaluates whether there is more than one agent logged into this queue.

CallType.CallType1.CallsRoutedToday > 100 - Evaluates whether more than 100 calls of this call type were routed today.

PQStep.PQ1.1.RouterAgentsLoggedIn > 1 - Evaluates whether there is more than one router agent logged into this queue for step 1.

CustomFunction(Call.PeripheralVariable1) > 10 - Evaluates whether this expression using a custom function returns a value greater than ten.

Step 12 Click **OK**. The step appears in the precision queue with the agent count. The agent count represents the number of configured agents that match the step criteria.

Note For a particular step, an equal or greater number of agents should be available to select from than in the previous step. If less agents are available to select from, a warning icon appears beside the agent count.

Step 13 To add an additional step, click **Add Step** and then return to step.

Note The **Add Step** button is disabled until you add at least one expression to the previous step. You can add up to 10 steps. After you reach 10 steps, the **Add Step** button is disabled. To delete a step, click the **X** icon.

Step 14 Click **Save**.

A message appears indicating that the precision queue was successfully saved and the summary page reappears.

Edit Precision Queue

Procedure

Step 1 In the summary view, navigate or search for the precision queue to edit.

Step 2 In the list, click the precision queue name. The page refreshes and the edit view appears.

Step 3 Complete required changes and click **Save**.

The page refreshes and the summary view appears. A message appears at the top of the page indicating whether or not the save was successful.

Delete Precision Queue

You cannot delete a precision queue that is referenced statically in any version of a saved script. Specifically, before you can delete a precision queue that is referenced statically in a script, you must remove the precision queue from every saved version of the script. If you reference a precision queue dynamically in a script and there are calls queued against the precision queue, you can delete the precision queue. Any calls queued against the deleted precision queue will be default routed.

Note When deleting a precision queue that is referenced by a dynamic precision queue node, this precision queue's calls will be default routed.

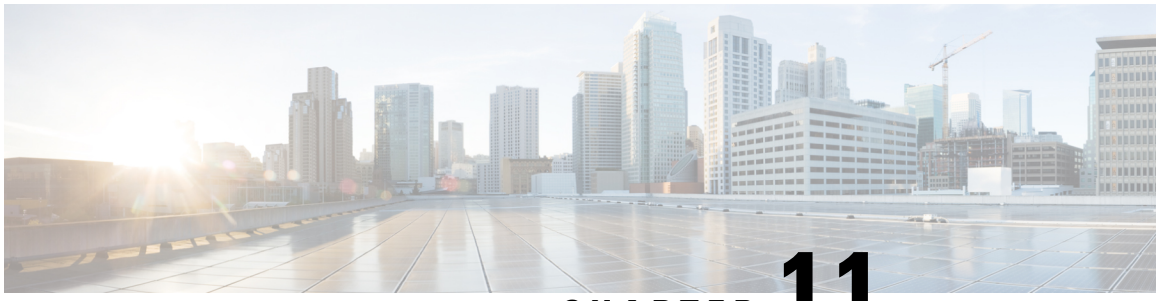
Procedure

Step 1 On the Precision Queue Summary page, select the precision queue to delete.

Step 2 Click the **X** icon.

You receive a prompt to confirm that you want to delete the precision queue.

Step 3 To delete the queue, click **Yes**. Otherwise, click **No**.



CHAPTER 11

Database Administration

Unified CCE Database Administration

When you install a new Logger, you create its central database. Create an HDS database on a real-time Administration & Data Server. When you create a database, you specify the size of its data or log files. The data files must be sufficient for all the data that you expect the database to hold. The size of the central and HDS databases depend on your call center traffic and your data retention requirements.

Note For more information on how to perform a manual configuration for integrating AWDB with ECE , see the section *Integrating ECE with Unified CCE* in the Enterprise Chat and Email Installation and Configuration Guide.

The local database (awdb) contains configuration and real-time data, if the Administration & Data Server role includes a real-time server. Because the real-time data in the local database (awdb) are constantly overwritten by new data, the database size remains fairly constant.

Over time, the size of your enterprise or your call volumes can change significantly. Therefore, you might need to resize the central and HDS databases to meet new requirements. You do not need to resize the local database (awdb). To resize the local database (awdb), use the ICM Database Administration (ICMDBA) tool.

The data in the central database and HDS database grow as they accumulate historical data and call detail records. The growth is directly related to the following factors:

- Size of the Unified ICM configuration; for example, how many services, skill groups, routes, and trunk groups are configured.
- Call rate; that is, how many calls per day the system software is handling.
- How long historical data is kept in the database.

The amount of configuration data directly affects the amount of historical data generated. The system software generates a new historical record every half hour for each service, skill group, route, trunk group, and so on, that is configured in the Unified ICM system.

You size and create the central and HDS databases after installing the system software. Use the Database Sizing Estimator applet for estimating the size of these databases, based on the expected usage.

If your configuration expands significantly or if you change the retention times for historical data, you might have to increase the size of the database. This increase might involve adding more disks to the system.

Historical Data

The system software initiates a purge process on the Logger once every day. By default, the purge process runs each night at 12:30 A.M. The purge process deletes records that are older than a specified number of retain days. When you set up the Logger using the Web Setup tool, you can modify the default retention time and purge schedule.

This table lists the *default* settings for retaining historical data.

Historical tables	Default retention time
Logger_Admin, Import_Rule_History, Persistent	30 days
Recovery	3650 days
All other historical tables	14 days

The following large historical tables are not purged by the system software but as a scheduled SQL Server Agent Job:

- Agent_Event_Detail
- Call_Type_SG_Interval
- Dialer_Detail
- Network_Event_Detail

- Route_Call_Detail
- Route_Call_Variable
- Termination_Call_Detail
- Termination_Call_Variable

Caution SQL Server Agent Jobs are installed and enabled during the Unified CCE install and upgrade procedure. Do not stop these jobs while the system software is active. If you plan to stop the Logger and Administration & Data Server-hds component services for maintenance for more than a day, manually disable the Microsoft SQL Server jobs using the SQL Server enterprise management tool. Later, after the services are started, re-enable the jobs.

Database Statistics

Maintaining accurate, up-to-date statistical details is essential to a well-run database environment and contributes to the optimizer's efficient handling of work load. In some SQL Server-based environments, it is not unusual to see users rely on the database itself to maintain statistics by using the Auto Create Statistics and Auto Update Statistics options. Setting these options in an AW environment (with its rapid data turnover) results in a considerable effort being expended in updating statistics. For that reason, users often schedule these options to run during off-peak hours. Because the database in the AW environment is nearly empty during off-peak times, however, statistics gathered then might not be as helpful as they would be when collected at other, busier times.

Another option to consider for gathering statistics is the creation of a SQL Server Agent job that periodically runs the Microsoft stored procedure sp_updatestats. The sp_updatestats procedure updates statistics as required for all user-defined and internal tables in the current database and can be run on an hourly basis if workload and environment permit.

Database Administration Tool

Unified CCE includes the ICMDBA tool (icmdba.exe) in the \icm\bin folder. This tool provides a central utility to administer the Unified ICM databases. Use this tool to:

- Create, edit, and delete central databases, local databases, and historical databases
- Resize database files
- Recreate databases
- Import and export Unified ICM configuration data to and from databases
- View database properties

In addition to these tasks, you can start or stop a server and do some limited SQL Server configuration.

Note Before using the ICMDBA tool, install the Unified CCE software. See the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide, for information on the Unified CCE installation.

Note The ICMDBA Import /Export feature works on Unified ICM configuration data only. To import or export Unified ICM historical data, use Microsoft's SQL Server Database Backup and Database Restore utilities.

You start the ICMDBA either by double-clicking **ICMDBA** in the Unified CCE Tools folder or by selecting **Start** > **Run** > **ICMDBA**.

The main window is a tree hierarchy displaying the Unified ICM database servers in the current domain.

Note If you cannot find the server you want in the main window, you can select any computer on your local network by choosing **File** > **Add Computer**.

Expanding the server name displays the Unified ICM instances that have databases on the server. Expanding the Unified ICM instance displays a specific Unified ICM node or nodes (Administration & Data Server and Logger) on machines that have databases for that instance. Expanding the node displays the databases associated with the node. Expanding the node database displays a list of the individual tables in the node database. Under databases are the table groups, and the final level lists the tables in the group.

You can create databases for instances with or without configured components. When an instance does not have configured components, database creation occurs under the instance within a component placeholder on the ICMDBA tree view.

To view the properties of a table, right-click the desired table in the list and select Properties from the context menu, or double-click the table in the list.

There are two ways to access the ICMDBA tool functions:

- From the main window, select a node or database from the tree and then select a function from the menu bar menu.
- Right-click a node or database to display a context menu.

Create Database with Configured Components

Use the Create function to create a database for an Administration & Data Server or Logger. You can only create one Logger database per side.

Procedure

Step 1 With the Unified CCE running, for the server and instance, select the node (Administration & Data Server or Logger) where you want to create the database.

Step 2 Select **Database** > **Create** from the menu bar (or click the right mouse button and select **Create**). The **Create Database** window is displayed.

Step 3 Enter the following information for the database:

- **DB Type**—Specify the type of database: **Outbound Option** for an outbound dialer, **Administration & Database Server** for a local database (awdb), or **Historical Data Server/Detail Data Server (HDS/DDS)** for Administration & Data Server machines. For a **Logger** device, the default database type is displayed (Logger side must be selected).
- **ICM Type**—Specify whether this system is a Unified ICM or Unified CCE, Unified ICMH, or CICM (Customer ICM) system.
- **Region**—Specify regional information where applicable.

Step 4 Select **Add**. This button invokes the **Add Device** window.

Use this window to create a new data file and a new log file for the selected database. Specify the disk drive letter and size in megabytes for each new file.

Note Move the database log file to a separate virtual drive. By default, both the log file and database data file are installed in `\MSSQL\DATA` on the virtual drive where you create the database. You can move the log file with SQL Server Management Studio.

Note By default, the newly created data file is set to "Automatically Grow," if it exceeds the initially specified size. You can modify this setting, and the maximum file size, with SQL Server Enterprise Manager. Verify on the **Files** page in SQL Server Enterprise Manager that the **Autogrowth** column shows:

- Data files automatically grow in 100-MB increments.
- Log files automatically grow in 10% increments.

Step 5 After you complete entering information in the **Create Database** window, select **Create** to close the window and create the database.

Create Database Without Configured Components

Use the Create function to create a database for an Administration & Data Server or Logger. You can only create one Logger database per side.

Note When an instance does not have any configured components, database creation occurs under the instance within a component placeholder.

Procedure

Step 1 With Unified CCE running, for the server and instance, select the instance where you want to create the database.

Step 2 Select **Database** > **Create** from the menu bar (or click the right mouse button and select **Create**). The **Select Component** dialog appears.

Step 3 Select the **Administration & Data Server**, **LoggerA**, or **LoggerB** component and select **OK**.

Step 4 If you select LoggerA or LoggerB, the **Select Logger type** dialog appears, allowing you to select **Enterprise**, **CICM**, or **NAM**. Select the logger type and select **OK**.
The **Create Database** window appears.

Step 5 Enter the following information for the database:

- **DB Type**—Specify the type of database: **Outbound Option** for an outbound dialer, **Administration & Database Server** for a local database (awdb), or **Historical Data Server/Detail Data Server (HDS/DDS)** for Administration & Data Server machines. For a **Logger** device, the default database type is displayed (Logger side must be selected).
- **ICM Type**—Specify whether this system is a Unified ICM or Unified CCE, Unified ICMH, or CICM (Customer ICM) system.
- **Region**—Specify regional information where applicable.

Step 6 Select **Add**. This button invokes the **Add Device** window.

Use this window to create a new data file and a new log file for the selected database. Specify the disk drive letter and size in megabytes for each new file.

Note Move the database log file to a separate virtual drive. By default, both the log file and database data file are installed in `\MSSQL\DATA` on the virtual drive where you create the database. You can move the log file with SQL Server Management Studio.

Note By default, the newly created data file is set to "Automatically Grow," if it exceeds the initially specified size. You can modify this setting, and the maximum file size, with SQL Server Enterprise Manager. Verify on the **Files** page in SQL Server Enterprise Manager that the **Autogrowth** column shows:

- Data files automatically grow in 100-MB increments.
- Log files automatically grow in 10% increments.

Step 7 After you have completed entering information in the Create Database window, select **Create** to close the window and create the database.

Delete a Database

Use the Delete function to delete an Administration & Data Server or Logger database.

Note When an instance does not have any configured components, component placeholders appear under that instance on the application tree view. If you delete the database, the component placeholders no longer appear.

Procedure

Step 1 With Unified CCE running, for the server, instance, and node (Administration & Data Server or Logger), select the database that you want to delete.

Step 2 Select **Database** > **Delete** from the menu bar.

Step 3 The **Delete Database** prompt appears. Select **Yes** to delete the database.

Step 4 Verify that you want to delete the database in the message box.

Step 5 Select **Close** to exit. Check the main window to verify that the database was deleted.

Expand a Database

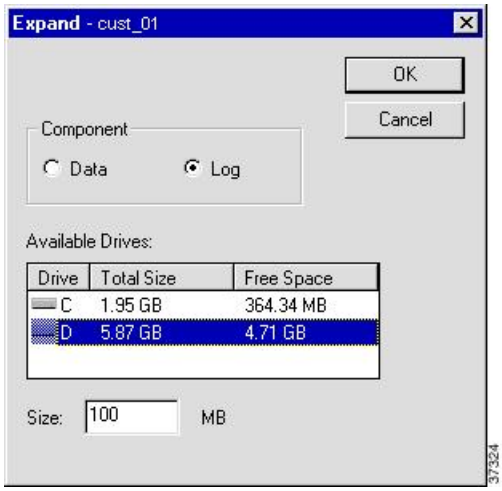
Use this function to add a new storage file.

Note ICMDBA allows a database to be expanded a maximum of 49 times (resulting in 50 segments). In the event that you reach this limit, you must either recreate the database or use SQL Enterprise Manager to modify the database.

Procedure

Step 1 For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to expand.

Step 2 Select **Database** > **Expand** from the menu bar (or click the right mouse button and select **Expand**). The **Expand** window appears:



Step 3 Use the window to adjust the size allocation on the database storage device, by completing the following fields:

- **Component**—Specifies whether the file is a data file or log file. Each database must have a file for each type of service.
- **Available Drives**—Specify the drive on which to create the database.
- **Size**—Specifies the size (in MB) of the storage. The field displays a default size, adjust the value as necessary.

Step 4 Select **OK** to expand the file and exit the screen.

Recreate a Database

Use the Recreate function to recreate a database. The procedure for recreating a database is similar to the procedure for creating a database.

Caution When you recreate a database, the information currently stored in the database is deleted.

Note When an instance does not have any configured components, database creation occurs under a component placeholder on the application tree view.

Procedure

Step 1 For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to recreate.

Step 2 Select **Database** > **Recreate** from the menu bar. The **Recreate** window appears.

Step 3 Enter the database information. See the online help for a description of the fields.

Step 4 Select **Create** to continue. A message is displayed asking if you are sure you want to recreate the database. Select **Yes** to continue the operation.

Step 5 The next **Recreate Database** window appears. Select **Start** to recreate the database. After the process completes, a message appears indicating the action was successful. Select **OK** and then select **Close** to exit.

View Database Properties

The ICMDBA tool allows you to view the properties of specified databases.

Procedure

Step 1 For the server, instance, and node (Administration & Data Server or Logger), select the database that you want to view.

Step 2 Select **Database** > **Properties** from the menu bar (or click the right mouse button and select **Properties**). The **Properties** window appears.

The screen display includes the following information:

- Instance name
- The database configuration
- The size and percentage used of the files
- Where the data and log files are stored

Step 3 After you finish viewing the database properties, select **Close** to exit the window.

View Table Properties

ICMDBA also allows you to view the properties of each table in the database.

Procedure

Step 1 Select and expand the database to display the tables of a database.

Step 2 Double-click the table you want to view. The **Table Properties** window appears.

Step 3 After you finish viewing the table properties, select **Close** to exit the window.

Import and Export Data

You can use Import/Export functions to move Unified ICM configuration data from one database to another.

Note The ICMDBA Import/Export feature handles Unified ICM configuration data only. To import or export Unified ICM historical data, use Microsoft's SQL Server Database Backup and Database Restore utilities.

Procedure

Step 1 For the server, instance, and node (Administration & Data Server or Logger), select the database from which you want to import or export data.

Step 2 Select **Data** > **Import** (or Export) from the menu bar. The **Import data to** (or Export) window appears.

Step 3 Check **Lockout Changes**, if you want to prevent changes to the database during the import or export operation.

Step 4 Check **Truncate Config Message Log**, if you want to truncate the Config_Message_Log table in the Logger database.

Note Truncating deletes the data and does not export the Config_Message_Log table.

Step 5 Set the **Data type** for the imported data.

Step 6 Indicate the path for the source/destination of the data.

Step 7 Select **Import** (or Export) to display the **Import** (or Export) dialog.

Step 8 Select **Start** to import (or export) the data. After the process completes, a message appears indicating that the action was successful. Select **OK** and then select **Close** to exit. You can select **Cancel** at any time to end the process.

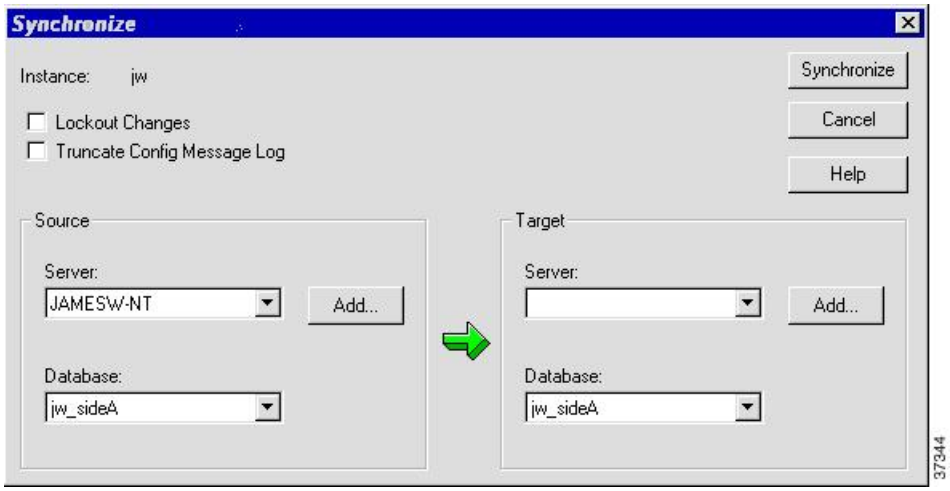
Synchronize Database Data

Use the Synchronize function to synchronize the configuration data of two Logger databases. This function does not synchronize the historical data.

Procedure

Step 1 For the server and instance, select the Logger database to synchronize.

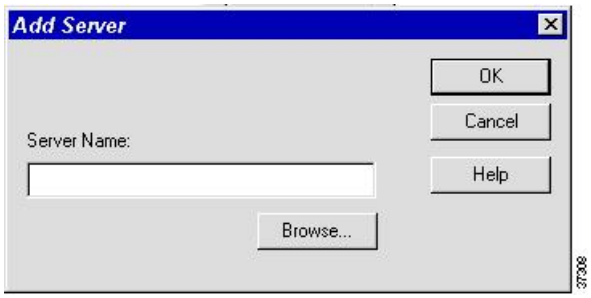
Step 2 Select **Data** > **Synchronize** from the menu bar. The **Synchronize** window appears:



Step 3 Check **Lockout Changes**, if you want to prevent changes to the database during the synchronize operation.

Step 4 Check **Truncate Config Message Log**, if you want to truncate the Config_Message_Log table in the Logger database.

Step 5 Select the server name and database for both source and target from the drop down lists. To select a server that is not on the drop down list, select **Add** and enter the server name in the **Add Server** box:



Step 6 Select **Synchronize**.

Step 7 A message box appears asking for confirmation. Select **OK** to continue.

Step 8 The next **Synchronize** window appears. Select **Start** to synchronize the data. After the process completes, a message appears indicating that the action was successful. Select **OK** and then select **Close** to exit. You can select **Cancel** at any time to end the process.

Configure a Database Server

ICMDBA allows you to start or stop a server and to do some limited server configuration.

To start or stop a server, select the node from the list and select **Server** > **Start/Stop** from the menu bar.

Note When you use the Configure option, the SQL Server, Administration & Data Server, and Logger restart automatically. However, when you use the Stop option from the Server menu, manually restart the Logger and Administration & Data Server from ICM Service Control.

Procedure

Step 1 Select the server and select **Server** > **Configure** from the menu bar. The **Configure** window appears.

Step 2 Use this window to modify the following SQL Server parameters:

- **User Connections**—Indicates the maximum number of users that can connect to SQL Server at one time.
- **Locks**—Indicates the maximum number of available locks.
- **Open Objects**—Indicates the maximum number of available open objects.

  Note User Connections, Locks, and Open Objects are "dynamically allocated" by SQL Server. Unified ICM does not allow you to change these options, so they are dimmed.

- **Open Databases**—Indicates the maximum number of available open databases.
- **Memory**—Indicates the amount of memory (in megabytes) allocated to SQL Server processing.

  Note You can configure a specific amount of memory instead of the SQL Server default of "Dynamic." Specifying a value of 0 sets the Memory setting to "Dynamic."

- **Recovery Interval**—This setting controls checkpoint frequency.
- **Max Async ID**—Indicates the maximum number of outstanding asynchronous disk input/output (I/O) requests that the entire server can issue against a file.

Step 3 After you are finished configuring the server, select **OK** to complete the operation or select **Cancel** to end the operation without making any changes.

Increase the size of the disk space for an existing virtual machine

For deployments of 4000 agents or more, you can increase the size of the virtual machine's (VM) disk space on your Windows server. To increase the size of the VM's disk space for 2000 agents deployment, follow these steps:

Before you begin

Plan for a maintenance window to increase the size of the disk space.

Procedure

Step 1 Power off the VM.

Step 2 Clone the VM or take a snapshot of the powered off VM.

Step 3 Change the size of the disk space, as required. Ensure that the disk format is set to Thick Provision Lazy Zeroed.

Step 4 Power on the VM.

Step 5 On the Windows server, go to **Server Manager** > **File and Storage Services** > **Volumes** > **Disks**.

Step 6 Modify the disk size and verify the changes.

Step 7 Delete the clone or snapshot of the old VM.

Database Sizing Estimator Tool

The Database Sizing Estimator tool enables you to perform database sizing tasks.

The Database Sizing Estimator estimates the storage requirements for a Cisco Unified ICM/CCE logger or HDS database. The tool bases the estimate ion information about the configuration of the environment (for example, the number of agents, skill groups, call types, and so on) and database retention days. You can supply initial values by loading values from your local Unified ICM database.

When values are updated in the Database Sizing Estimator, the application recalculates its totals. This update enables you to immediately see the affects of each change as it is made, with the values displayed in a spreadsheet. The tool enables you to engage in what-if scenarios to see the effects that various changes have on the database sizing requirements.

The Database Sizing Estimator allows you to save the values as an XML file on your local machine. At any time, you can load the saved XML file back into the Database Sizing Estimator, so you can continue revising your estimates.

Cisco Unified ICM/CCE Database Retriever Dialog

The Cisco Unified ICM/CCE Database Retriever dialog, which you access from the Database Sizing Estimator tool, queries the existing database and registry configuration. The Database Sizing Estimator tool then uses this data to provide starting values, which you can modify.

To access the **Database Retriever** dialog, select **Load from DB** in the Database Sizing Estimator tool on your local machine.

Note Cisco Unified ICM/CCE Database Retriever can retrieve the configuration and retention information from any Unified ICM/CCE system containing a Logger or Historical Data Server (HDS) database. The Database Sizing Estimator can calculate a database size for a newer schema other than the deployment to which the Database Sizing Estimator is connected.

Start Database Sizing Estimator

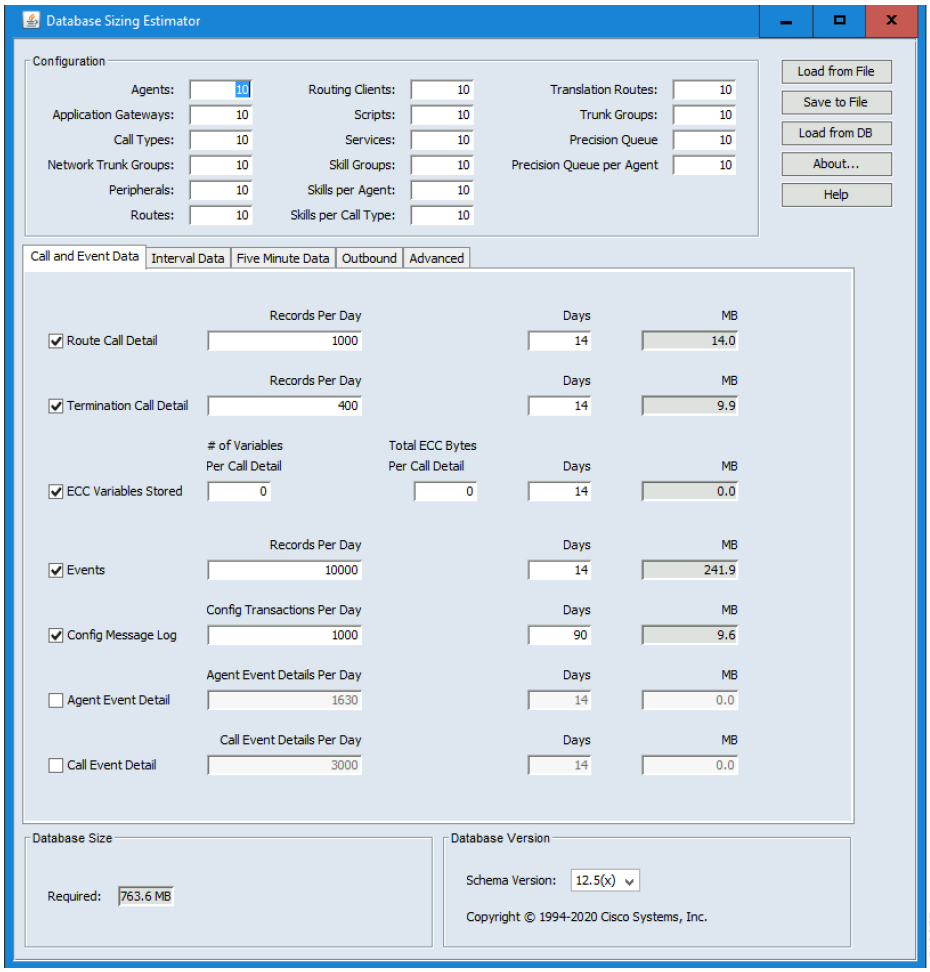
The following steps describe how to start the Database Sizing Estimator.

Note For Database Sizing Estimator field-level descriptions, see the online help.

Procedure

Step 1 Open the Database Sizing Estimator tool by selecting **Database** > **Estimate** in the ICMDBA tool.

Step 2 The Cisco Unified ICM/CCE Database Sizing Estimator window appears:



Step 3 The window displays initial default values for all fields. As you change the field values, the database size requirements update automatically. You can load values from a previous version or from the **Cisco Unified ICM/CCE Database Retriever** dialog by selecting **Load from File** to load an external XML data file.

Estimate Database Size

Note Steps 1–3 in this procedure only apply when using existing databases.

Procedure

Step 1 Use your existing database as the starting point. Select **Load from DB** in the **Database Sizing Estimator** main window. The **Cisco Unified ICM/CCE Database Retriever** dialog appears.

Step 2 Select the database you want to use as the starting point for your sizing estimates.

Step 3 Select **Retrieve**.
The fields in the **Database Sizing Estimator** main window auto-populate with the information from the selected database.

Step 4 Modify the database information depending on your scenario. As changes are made, the **Database Size Required** value changes.

Step 5 Save your work in progress by selecting **Save to File**.

Administration and Data Server with Historical Data Server Setup

There are two ways to set up a Historical Data Server (HDS) VM:

- The instance is created in the domain, but not already added.
- The instance is created in the domain and is already added.

Set Up HDS and Add Instance

Procedure

Step 1 Run the Cisco Unified ICM/Contact Center Enterprise (if you have not run it already) on the local machine.

Step 2 Run the Web Setup tool for that machine (in a browser, from anywhere). Under **Instance Management**, select **Add** and add the instance.

Step 3 Run the ICMDBA tool on the local machine. Create the Historical Data Server/Detail Data Server database.

Step 4 Return to the Web Setup tool. Under **Component Management**, select **Add** on the Administration & Data Server list page, then follow the instructions in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide. If you did not perform step 3, the Administration & Data Server **Add** wizard does not allow you to finish this procedure until you create an HDS database.

What to do next

Use the Database Sizing Estimator tool to determine the size of the database and then use the ICMDBA tool to create the database.

Set Up HDS from Added Instance

Procedure

Step 1 Run the Cisco Unified ICM/Contact Center Enterprise Installer (if you have not run it already) on the local machine.

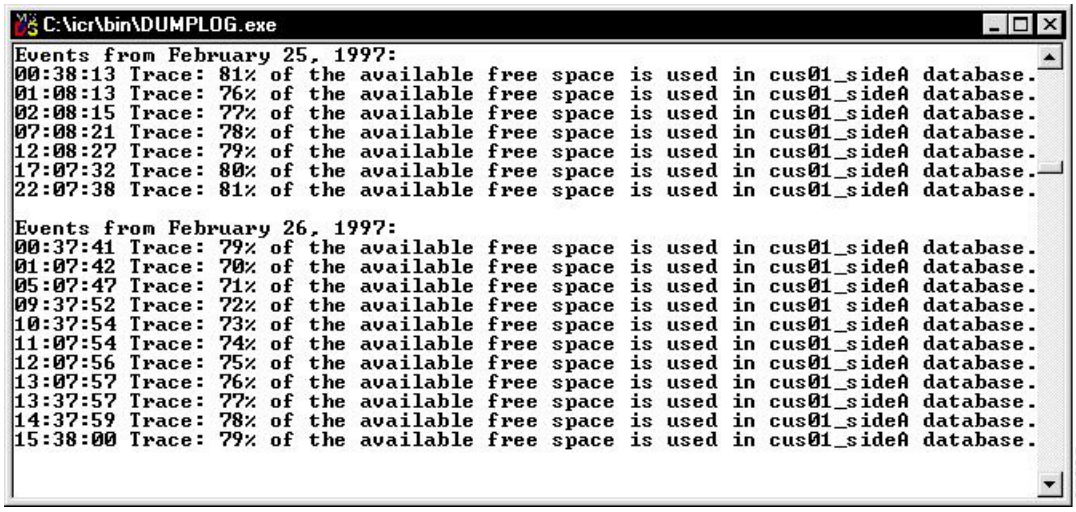
Step 2 In the Web Setup tool, under **Component Management**, select **Add** on the Administration & Data Server list page, then follow the instructions in the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide. If you did not perform step 1, the Administration & Data Server **Add** wizard does not allow you to finish this procedure until you create an HDS database.

What to do next

Use the Database Sizing Estimator tool to determine the size of the database and then use the ICMDBA tool to create the database.

Database Size Monitoring

Regularly monitor the space used by the central database and transaction logs. You can monitor database size by viewing the Logger's per-process log files. The per-process log files contain information on Logger and database activity, as this example log file illustrates:



The Logger logs events and trace messages that show the percentage of space used in the database. These files are stored in a `\logfiles` subdirectory in the Logger's folder (la or lb). You can view the Logger's per-process log files by using the Unified ICM dumplog utility.

When the database becomes 80 percent full, the Logger logs an EMS warning message to the central database. The “80 percent full” warning message might also immediately be sent to your Unified ICM network management station through SNMP or SYSLOG.

Note See the Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise for more information on using the dumplog utility.

If you decide that you need more database space, contact your Unified ICM support provider.

System Response When Database Nears Capacity

The system software has automatic checks to prevent the central database from becoming full:

- **Warning message**—When the central database begins to approach its capacity, the system software issues a warning message. By default, this warning occurs when the database is 80% full, but you can configure this value. Warning messages trigger an event that is registered in AlarmTracker, which the console window displays in an EMS trace message.
- **Purge Adjustment**—Purge Adjustment automatically deletes the oldest historical data when the database usage exceeds 80% threshold or when the central or HDS database nears its capacity. However, purge adjustment does not happen immediately. It happens at the default scheduled purge time (00:30 AM), or at the time that you have specified for the scheduled purge to happen.

  By default, purge adjustment occurs when the database is 80% full, but you can specify the percentage when you set up the Logger.

  If the historical databases for the Logger, AW-HDS-DDS, AW-HDS, and HDS-DDS are not adequately sized, the purge adjustment feature is activated when the database usage exceeds the threshold. Use the **Database Sizing Estimator** tool to size your database requirements.

  Note The purge adjustment feature affects performance of the Unified CCE system. The high CPU and disk usage due to purge adjustment could affect component performance including failures.

  See the Cisco Unified Contact Center Enterprise Installation and Upgrade Guide for more on purging information from databases.
- **Emergency/Automatic Purge**—By default, the system automatically deletes the oldest historical data from all historical tables when the database exceeds 90% usage capacity.

The automatic purge ensures that the database can never become full. But, the purge means that you can lose older historical data.

Allocation of More Database Space

If the central database is growing too large, you can allocate more space. If you require more space in the central database, back up the primary database before you add more space. Your Unified CCE support provider might have options for allocating more space.

Initialize Local Database (AWDB)

Usually, you do not need to initialize the local database (awdb), because initialization happens automatically during its creation. If you ever need to initialize the local database after its creation, you can do so.

Procedure

Step 1 Double-click **Initialize Local Database** within the Administration Tools folder. The **Initialize Local Database** main window appears.

Step 2 Select **Start** to transfer the data. As data is copied, the screen displays the number of rows processed for each table.

Step 3 After the transfer is complete, select **Close** to exit.

General Database Administration

Because Unified ICM is a mission-critical application that runs 24 hours a day, the system software takes care of many routine administration tasks automatically. In general, the system software retains control of most of the database administration functions in order to keep external interference to a minimum.

The Unified ICM administrator might perform several optional Unified ICM administration tasks:

- Setting networking options
- Monitoring Logger activity
- Backing up the central database
- Restoring the central database from a backup
- Comparing databases
- Resynchronizing databases

Note To conserve system resources, minimize all Unified ICM process windows before configuring your system.

Built-In Administration

The system software maintains a database on each side of the Central Controller and the local database (awdb). Each database consists of a group of interrelated tables. As you add or update data in the database, ensure that

logical relationships are maintained. For example, if you delete a trunk group, do not leave trunks in the database that reference that trunk group. If you do, the integrity of the database is broken.

Configuration Manager prevents you from making certain changes that disrupt the integrity of the data in the database. However, it cannot prevent all such changes. Usually, if data integrity in the local database (awdb) is temporarily disrupted, no major problems occur. However, integrity problems in the central Unified CCE database could cause errors in system processing.

Note To protect the integrity of the Unified CCE databases, do not use third-party tools to modify them. These tools do not protect against disruptions of database integrity. (You can use third-party tools to view Unified ICM data.)

When your Unified CCE support provider installs the Unified CCE system, they perform integrity checks to make sure that the database is configured correctly. After that, the system software maintains the integrity of the central database. You do not need to manually check the integrity of the Unified CCE central database. If you ever have a problem with data integrity in the central database, the problem is most likely a software problem that your Unified CCE support provider needs to address.

Caution Manual integrity checks of the central database must involve your Unified CCE support provider. Do not run the DBCC CHECKDB procedure on the central database with the Unified CCE system running. This procedure stops the Logger.

Check AWDB Data Integrity

You can manually check the integrity of data in the local database (AWDB). Configuration Manager provides a Check Integrity option under the Administer menu. Configuration Manager allows you to select the checks that you need to run.

The specific data integrity check procedures are listed in the following table:

Table 6: Local Database Data Integrity Check Procedures

Procedure	Description
Null	Checks the database for the value NULL in fields that must not have the value NULL. Checks if the value of the RoutingClient.PeripheralID is NULL for the routing clients associated with the NIC.
Targets	Checks for appropriate relationships among peripherals, targets at peripherals (services, skill groups, agents, and translation routes), trunk groups, network targets, announcements, and peripheral targets.
Routes and Numbers	Checks if the ID fields cross-referenced from several tables correspond to the existing records.
Scripts	Checks for valid cross-references among scripts, call types, and dialed numbers.

Procedure	Description
Enterprise	Checks for valid cross-references among enterprise services and services, and between enterprise skill groups and skill groups. Also performs several other checks on skill groups, trunks, and so on.
Domain Adherence	Checks for valid relationships between agents and skill groups, between skill groups and services, between labels and routing clients, between dialed numbers and routes, and between peripherals and routing clients.
Names	Checks for invalid characters in enterprise names (EnterpriseName field) in various database tables. Enterprise names provide unique character-string names for objects in the Unified ICM configuration.
Miscellaneous	Checks rules for Outbound Option Configuration.

For more information on the specific fields checked by these procedures, see the online help for the Configuration Manager tool.

Procedure

Step 1 Invoke Configuration Manager by double-clicking its icon in the Administration Tools folder.

Step 2 Select **Configure ICM** > **Administration** > **Integrity Check** from the menu bar. The **Integrity Check** dialog box appears.

Step 3 Select specific checks to run, or select All to perform all the checks.

Step 4 Select **Start** to perform the checks. If any integrity problems are found, the Configuration Manager displays a message describing the problems.

Step 5 After you perform all the checks you want, select **Done** to dismiss the **Integrity Check** dialog box.

Logger Events

You can view recent Logger activity by viewing the Logger's per-process log files. Per-process log files document events for the specific processes running on a computer. These files are useful in diagnosing problems with processes on the Logger (and on other nodes in the Unified ICM system).

You can also view Logger event data in the central database. The Event Management System (EMS) logs events to the central database. Be especially aware of Error and Warning events generated by the Logger. For example, the system software logs a Warning event when the central database becomes 80% full.

See the Serviceability Best Practices Guide for Cisco Unified ICM/Contact Center Enterprise for more information on viewing the per-process log files and central database event data.

Database Networking Support

You can use the SQL Server Setup program to specify which network protocols the database manager supports.

The correct order and states are:

1. **Shared Memory**—Enabled
2. **Named Pipes**—Enabled
3. **TCP/IP**—Enabled
4. **VIA**—Disabled

See the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise* http://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html for detailed information about installing SQL Server. For more information about database networking, see the Microsoft documentation for Microsoft SQL Server.

Database Backup and Restore

A database can be lost or corrupted for several reasons. Because you cannot protect against all these reasons, you must have a backup strategy in place. This backup strategy is especially important if you have a nonredundant central database configuration. However, even for a redundant system, you still need to perform backups to protect against software problems that corrupt both sides of the system.

The commonly used database backup strategies are:

- Regularly scheduled database backups
- Mirrored disk configurations
- Redundant Array of Inexpensive Disks (RAID) configurations

Although the last two strategies might decrease system performance, they have the advantage of not requiring manual intervention. However, while these configurations protect against disk drive failure and bad media, they might not protect against some software errors.

In a single database configuration, ensure protection against all types of errors. To protect your data, regularly back up the central database with the SQL Administrator tool provided with SQL Server.

When you restore a database, you can only restore up to the last backup. Any transactions after that backup are lost. In single database configurations, daily backups are required to ensure maximum data protection.

Note You must back up the entire database at each backup interval. The system software does not support the use of transaction log dumps as incremental backups.

For general information about developing a backup strategy, including the use of mirrored disks, see *Microsoft's SQL Server System Administrator's Guide*. For specific information about backing up a database using SQL Administrator, see *Microsoft's SQL Administrator User's Guide*.

Database Recovery Models 12 5

When you install an ICM and create Logger, HDS, BA, or AWDB, the ICMDBA tool automatically sets the database recovery model to Simple. The Simple recovery model is required for Unified CCE data recovery mechanism.

For more information, see Microsoft documentation.

Database Comparison

For diagnostic purposes, you can check that two databases have the same data in a specific table. For example, you can check that the ICM_Locks table contains the same data on both sides of a Central Controller. The tool `dbdiff.exe` performs this type of check. Its syntax is as follows:

```
dbdiff database1.table@host1 database2.table@host2
```

For example:

```
dbdiff cust1_sideA.ICM_Locks@geoxyzlgra cust1_sideB.ICM_Locks@geoxyzlgrb
```

The batch script `diffconfig.bat` invokes **dbdiff** for various tables to automatically compare two Unified ICM databases. Its syntax is as follows:

```
diffconfig database1 host1 database2 host2
```

For example:

```
diffconfig cust1_sideA geoxyzlgra cust1_sideB geoxyzlgrb
```

Database Resynchronization

You might occasionally need to repair corrupt configuration data on the Logger database on one side of a redundant Unified ICM by copying the configuration data on Logger database from the other side. You can synchronize the configuration data on the databases using either the DOS Command window or the ICM Database Administration (ICMDBA) tool.

The ICMDBA synchronize process involves dropping the targeted side data and copying the data from the source. For example, if you are synchronizing side B data to side A data, the side B data is replaced with the data stored in side A. For more information, see Synchronize Database Data, on page 97.

Note Perform these procedures in a maintenance window.

Synchronize Configuration Data between Loggers from Command Window

Procedure

Step 1 Stop the Logger for the target database, if that Logger is running.

Step 2 In a DOS Command window on the VM for that Logger, change to the `\icm` directory.

Step 3 Run the following command: **install\syncloggers *<Source_logger_server> <Source_logger_database> <Target_logger_server> <Target_logger_database>***.

Step 4 When prompted, Type **Y** to continue, upon which configuration of target database will be deleted and synced with source database.

What to do next

When the command is complete, restart the Logger on the target server.

Change Limits for Calls Per Second to Support 36000 Agents

Each Unified CCE instance database contains Configuration Limit scalability records. Supporting up to 36000 active agents requires the modification of the following records:

- Call Per Second rate
- Deployment Max CPS

You can change the values for these records using the Configuration Limit tool, which modifies the Configuration_Limit Database table.

The Configuration Limit tool is a command-line utility tool from the bin directory of all Unified ICM and Unified CCE Administration & Data Servers. You must have privileges for the Setup or Config Groups in the Active Directory for the chosen Unified CCE instance.

Note Using the Configuration Limit tool, you can only change the ConfigLimitCurrentValue. You cannot change the ConfigLimitDefaultValue.

Procedure

Step 1 In the Windows Run dialog, type **`configlimit`**, and then click **Enter**.

Note Run the Configuration Limit tool on the same machine as the Distributor for the instance that you want to configure. If there are several instances of the Administration & Data Server on the Distributor machine, use the Select Administration Server tool to select the instance to configure.

Step 2 To view currently configured parameter limits, run the following command: `cl /show`

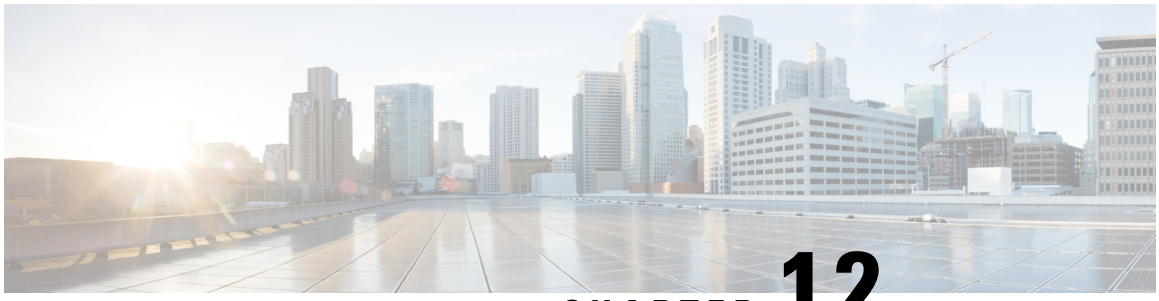
Step 3 To change the calls per second limit, run a command in the following format: `cl /id [ConfigLimitID] /value [ConfigLimitCurrentValue][/update]`

Where

- ConfigLimitID valid values are:
  - 12—CPS_CAPACITY
  - 14—DEPLOYMENT_MAX_CAPACITY
- ConfigLimitCurrentValue is the parameter limit.

To set the maximum supported Calls per Second capacity support for congestion control: `cl /id 12 /value 310 /update`

To set the maximum supported Calls per Second for this Deployment Type: `cl /id 14 /value 310 /update`



CHAPTER 12

Single Sign-on Administration

Single Sign-on Administration

Set up the System Inventory for Single Sign-On

Set up the System Inventory before configuring the Cisco Identity Service (Cisco IdS) and the components for single sign-on. By default, the System Inventory displays a list of all AWs, Routers, and Peripheral Gateways in the deployment.

The Principal AW (Admin Workstation) is responsible for managing background tasks that are run periodically to sync configuration with other solution components, such as SSO management, Smart Licensing, etc.

Select the Principal AW to manage to register the components with the Cisco IdS and enabling them for SSO. Add the remaining SSO-capable machines to the System Inventory, and select the default Cisco IdS for each of the SSO-capable machines.

Procedure

Step 1 In Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Set the Principal AW:

a) Click the AW that you want to be the Principal AW.

Note If the AW is coresident with the Router, you can set the Principal AW on the Router.

You can only specify one Principal AW for each Unified CCE system.

The **Edit AW** popup window opens.

b) Check the **Principal AW** check box on the General tab.

c) Enter the Unified CCE Diagnostic Framework Service domain, username, and password.

These credentials must be for a domain user who is a member of the Config security group for the instance. These credentials must be valid on all CCE components in your deployment (Routers, PGs, AWs, and so on).

d) Click **Save**.

Step 3 Add the SSO-capable machines to the System Inventory:

a) Click **New**.
The **Add Machine** popup window opens.

b) From the **Type** drop-down, select one of the following types of machines:

- **Finesse Primary**
- **CUIC, LD, IdS Publisher**, for the coresident Unified Intelligence Center, Live Data, and Cisco IdS machine available in the 2000 agent or Progger (Lab only) reference design
- **Unified Intelligence Center Publisher**, if you're using a standalone Unified Intelligence Center
- **Identity Service Primary**, if you're using a standalone Cisco IdS

c) In the **Hostname** field, enter the FQDN, IP address, or hostname of the machine.

Note If you don’t enter the FQDN, the system converts the value you enter to FQDN.

d) Enter the machine's Administration credentials.

e) Click **Save**.
The machine and its related Subscriber or Secondary machine are added to the System Inventory.

f) Repeat this procedure to add all of the SSO-capable machines in the deployment.

Step 4 Select the default Identity Service for each of the following machines:

- All Unified CCE AW servers
- Finesse Primary and Secondary
- Unified Intelligence Center Publisher and Subscriber

Note If you're using a coresident CUIC, LD, Ids Publisher and Subscriber, you don't need to set the default Cisco IdS for those machines.

In a standalone deployment, select the Cisco IdS that's deployed on the same Data Center Side (A or B) as the machine that you're configuring. For example, in the Reference Deployment:

- Select the Identity Service Publisher (IdS A) for AW-HDS-DDS 1, AW-HDS 3, Finesse 1 Pub, Finesse 2 Pub, CUIC Pub, and CUIC Sub 1.
- Select the Identity Service Subscriber (Ids B) for AW-HDS-DDS 2, AW-HDS 4, Finesse 1 Sub, Finesse 2 Sub, CUIC Sub 2, and CUIC Sub 3.

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

a) Click a machine to open the **Edit Machine** popup window.

b) Click the Search icon next to **Default Identity Service** to open the **Select Identity Service** popup window.

c) Enter the machine name for the Cisco IdS in the Search field and choose the Cisco IdS from the list.

d) Click **Save**.

What to do next

Be sure to update the System Inventory if you change your deployment:

- If you add or remove contact center solution components from your deployment, make the corresponding changes in the System Inventory.
- If you add or remove Cisco Identity Service machines or coresident CUIC-LD-IdS machines, update the System Inventory appropriately and reconfigure the Cisco IdS. Reassociate the components with a default Cisco IdS.

Configure the Cisco Identity Service

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

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

Note If you are working with a Cisco IdS cluster, perform these steps on the Cisco IdS primary publisher node.

Be sure that the Principal AW is configured and functional before using the **Features** > **Single Sign-On** tool in Unified CCE Administration.

Procedure

Step 1 In Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

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

Step 2 Click **Identity Service Management**.

Result:

The Cisco Identity Service Management window opens.

Step 3 Enter your user name, and then click **Next**.

Step 4 Enter your password, and then click **Sign In**.

The Cisco Identity Service Management page opens, showing the **Nodes**, **Settings**, and **Clients** icons in the left pane.

Step 5 Click **Nodes**.

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

Step 6 Click **Settings**.

Step 7 Click **IdS Trust**.

Step 8 To begin the Cisco IdS trust relationship setup between the Cisco IdS and the IdP, click **Download Metadata File** to download the file from the Cisco IdS Server.

Step 9 Click **Next**.

Step 10 To upload the trusted metadata file from your IdP, browse to locate the file.
The **Upload IdP Metadata** page opens and includes the path to the IdP. When the file upload finishes, you receive a notification message. The metadata exchange is now complete, and the trust relationship is in place.

Step 11 Clear the browser cache.

Step 12 Enter the valid credentials, when page is redirected to IdP.

Step 13 Click **Next**.
The **Test SSO Setup** page opens.

Step 14 Click **Test SSO Setup**.
A message appears telling you that the Cisco IdS configuration has succeeded.

Step 15 Click **Settings**.

Step 16 Click **Security**.

Step 17 Click **Tokens**.
Enter the duration for the following settings:

- **Refresh Token Expiry** -- The default value is 10 hours. The minimum value is 2 hours. The maximum is 24 hours.
- **Authorization Code Expiry** -- The default value is 1 minute, which is also the minimum. The maximum is 10 minutes.
- **Access Token Expiry** -- The default value is 60 minutes. The minimum value is 5 minutes. The maximum is 120 minutes.

Step 18 Set the **Encrypt Token** (optional); the default setting is **On**.

Step 19 Click **Save**.

Step 20 Click **Keys and Certificates**.
The **Generate Keys and SAML Certificate** page opens and allows you to:

- Regenerate the **Encryption/Signature key** by clicking **Regenerate**. A message appears to say that the Token Registration is successful and advises you to restart the system to complete the configuration.
- Regenerate the **SAML Certificate** by clicking **Regenerate**. A message appears to say that the SAML certificate regeneration is successful.

Step 21 Click **Save**.

Step 22 Click **Clients**.
The **Clients** page identifies the existing Cisco IdS clients, providing the client name, the client ID, and a redirect URL. To search for a particular client, click the Search icon above the list of names and type the client's name.

Step 23 To add a client:

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

Step 24 To edit or delete a client, highlight the client row and click the ellipses under **Actions**. Then:

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

Step 25 Click **Settings**.

Step 26 From the **Settings** page, click **Troubleshooting** to perform some optional troubleshooting.

Step 27 Set the local log level by choosing from **Error**, **Warning**, **Info** (the default), **Debug**, or **Trace**.

Step 28 To receive errors in Syslog format, enter the name of the Remote Syslog Server in the Host (Optional) field.

Step 29 Click **Save**.

You can now:

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

Register Components and Set Single Sign-On Mode

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

Before you begin

- Configure the Cisco Identity Service (Cisco IdS).
- Disable popup blockers. It enables viewing all test results correctly.
- If you are using Internet Explorer, verify that:
  - It is not in the Compatibility Mode.
  - You are using the fully qualified domain name of AW to access the CCE Administration (for example, **https://<FQDN>/cceadmin**).

Procedure

Step 1 In the Unified CCE Administration, navigate to **Features** > **Single Sign-On**.

Step 2 Click the **Register** button to register all SSO-compatible components with the Cisco IdS.

The component status table displays the registration status of each component.

If a component fails to register, correct the error and click **Retry**.

Step 3 Click the **Test** button. When the new browser tab opens, you may be prompted to accept a certificate. In order for the page to load, accept any certificates. Then, when presented with a log in dialog, log in as a user with SSO credentials.

The test process verifies that each component has been configured correctly to reach the Identity Provider, and that the Cisco IdS successfully generates access tokens. Each component that you are setting up for SSO is tested.

The component status table displays the status of testing each component.

If a test is unsuccessful, correct the error, and then click **Test** again.

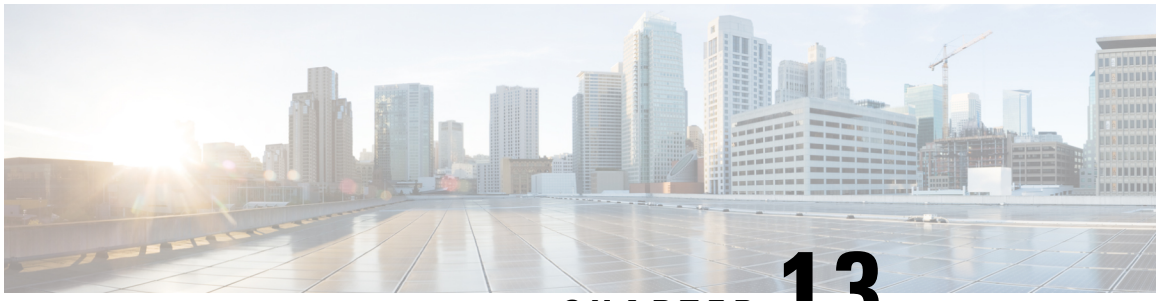
Test results are not saved. If you refresh the page, run the test again before enabling SSO.

Step 4 Select the SSO mode for the system from the **Set Mode** drop-down menu:

- Non-SSO: This mode disables SSO for all agents and supervisors. Users log in using existing Active Directory-based local authentication.
- Hybrid: This mode allows you to enable agents and supervisors selectively for SSO.
- SSO: This mode enables SSO for all agents and supervisors.

The component status table displays the status of setting the SSO mode on each component.

If the SSO mode fails to be set on a component, correct the error, and then select the mode again.



CHAPTER 13

Web Setup

Session Timeout

Timeout	Description	Range Values	Default Value
Idle Timeout	The time interval for which the session remains active without any activity.	5 minutes to 30 minutes.	30 minutes
Absolute Timeout	The maximum time interval for which the session remains active.	Maximum 1440 minutes (24 hours).	1440 minutes

Implementing Session Timeouts

Implement the session timeout configurations in the `Web.xml` file.

Procedure

Step 1 Implement Idle Timeout using the session configuration:

```
<!-- Session Configuration -->
<session-config>
                <session-timeout>30</session-timeout>
</session-config>
```

Step 2 Implement Absolute Timeout using the session filter:

```
<filter>
           <filter-name>sessionFilter</filter-name>
           <filter-class>com.cisco.icm.websetup.filter.SessionFilter</filter-class>
           <init-param>
                              <param-name>maxPeriod</param-name>
                              <param-value>1440</param-value>
```

```
            </init-param>
</filter>
```